ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58412— 2019

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Угрозы безопасности информации при разработке программного обеспечения

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Акционерным обществом «Научно-производственное объединение «Эшелон» (АО «НПО «Эшелон»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 мая 2019 г. № 204-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

Содержание

Введение

Настоящий стандарт входит в комплекс стандартов, направленных на достижение целей, связанных с предотвращением появления и/или устранением уязвимостей программ, и содержит систематизированный перечень угроз безопасности информации, которые могут возникать при разработке программного обеспечения.

Информация, представленная в настоящем стандарте, может быть использована разработчиком программного обеспечения при выборе (определении) и реализации мер по разработке безопасного программного обеспечения, установленных ГОСТ Р 56939.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Угрозы безопасности информации при разработке программного обеспечения

Information protection. Secure software development. Software development life cycle threats

Дата введения — 2019—11—01

1 Область применения

Настоящий стандарт устанавливает перечень и содержит описание угроз безопасности информации, которые могут возникать при разработке программного обеспечения. Настоящий стандарт предназначен для разработчиков и производителей программного обеспечения и применяется совместно с ГОСТ Р 56939. Информация о мерах по разработке безопасного (защищенного) программного обеспечения, установленных ГОСТ Р 56939, реализация которых способствует нейтрализации угроз безопасности информации при разработке программного обеспечения, приведена в приложении А.

Перечень и описание угроз безопасности информации, представленные в настоящем стандарте, могут использоваться для определения угроз безопасности, актуальных для среды разработки программного обеспечения и разрабатываемого программного обеспечения. В некоторых случаях, например, в процессе разработки программ для ЭВМ с открытым кодом или при использовании программ для ЭВМ с открытым кодом в составе разрабатываемого ПО разработчик может принять осознанное решение об отсутствии необходимости сохранения конфиденциальности определенных компонентов ПО, что соответствующим образом может отразиться на результатах идентификации и оценки угроз безопасности информации: угрозы нарушения конфиденциальности информации, содержащейся в указанных компонентах ПО будут являться неактуальными.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 19781 Обеспечение систем обработки информации программное. Термины и определения

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 51275 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 54593 Информационные технологии. Свободное программное обеспечение. Общие положения

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р ИСО 10007 Менеджмент организации. Руководящие указания по управлению конфигурацией

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Издание официальное

ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 27000, ГОСТ Р ИСО 10007, ГОСТ 19781, ГОСТ Р 50922, ГОСТ Р 51275, ГОСТ Р 54593, ГОСТ Р 56939, а также следующие термины с соответствующими определениями:

3.1 **инструментальное средство:** Программа, используемая как средство разработки, тестирования, анализа, производства или модификации других программ или документов на них.

3.2 **исходный код программы:** Программа в текстовом виде на каком-либо языке программирования.

3.3 **среда разработки программного обеспечения:** Среда, в которой осуществляется разработка программного обеспечения.

4 Общие положения

4.1 При реализации требований ГОСТ Р 56939 разработчиком безопасного программного обеспечения (ПО) должен быть определен перечень мер, подлежащих реализации при его разработке в целях предотвращения появления и устранения уязвимостей программ в процессах их жизненного цикла. Выбор и уточнение мер по разработке безопасного ПО должен основываться на результатах проводимого разработчиком ПО анализа угроз безопасности информации, в результате которого должны быть определены актуальные для среды разработки ПО угрозы безопасности информации. Угрозы безопасности информации при разработке ПО, представленные в настоящем стандарте, могут являться основой для проведения анализа угроз безопасности информации конкретной среды разработки ПО.

4.2 Перечень угроз безопасности информации, приведенный в настоящем стандарте, является специфичным для процессов жизненного цикла ПО, в ходе которых в ПО могут быть внедрены уязвимости программы или нарушена конфиденциальность информации, потенциально способствующей выявлению недостатков ПО и уязвимостей программы. Угрозы безопасности информации, приведенные в настоящем стандарте, являются антропогенными. В настоящем стандарте не рассматриваются угрозы безопасности информации, связанные со стихийными бедствиями, природными явлениями и утечкой информации по техническим каналам.

4.3 Перечень угроз безопасности информации не является исчерпывающим и может быть дополнен и (или) уточнен в процессе идентификации угроз безопасности информации для конкретной среды разработки ПО.

4.4 В качестве источников угроз безопасности информации при разработке ПО могут выступать:

- лица (нарушители), осуществляющие преднамеренные или непреднамеренные действия, направленные на внедрение в ПО уязвимостей программы или нарушение конфиденциальности информации, потенциально способствующей выявлению недостатков ПО и уязвимостей программы;

- инструментальные средства, применяемые при разработке ПО, алгоритм работы которых может стать причиной внедрения в ПО уязвимостей программы.

Примечание — К инструментальным средствам относятся, например, трансляторы, компиляторы, прикладные программы, используемые для проектирования и документирования, редакторы исходного кода программ, отладчики, интегрированные среды разработки.

Непреднамеренные угрозы безопасности информации при разработке ПО возникают из-за неосторожности или неквалифицированных действий работников разработчика ПО и связаны с недостаточной осведомленностью работников в области защиты информации и разработки безопасного ПО.

4.5 С учетом возможностей по доступу к среде разработки ПО нарушителей в настоящем стандарте подразделяют на два типа:

- внешние нарушители — лица, не имеющие доступа к среде разработки ПО и реализующие угрозы безопасности информации из выделенных (ведомственных, корпоративных) сетей связи, внешних сетей связи общего пользования;
- внутренние нарушители — лица, имеющие постоянный или разовый доступ к среде разработки ПО.

Внутренние нарушители могут реализовывать угрозы безопасности информации при разработке ПО путем:

- влияния на процессы жизненного цикла ПО;
- осуществления преднамеренных или непреднамеренных действий в отношении отдельных объектов среды разработки ПО, в том числе элементов конфигурации, выполняя санкционированный доступ;
- осуществления преднамеренных действий в отношении отдельных объектов среды разработки ПО, в том числе элементов конфигурации, выполняя несанкционированный доступ.

Внешние нарушители могут реализовывать угрозы безопасности информации при разработке ПО путем удаленного доступа (из внешних сетей связи общего пользования) к объектам среды разработки ПО, в том числе элементам конфигурации, выполняя несанкционированный доступ. Внешние нарушители для повышения своих возможностей по доступу к объектам среды разработки ПО могут вступать в сговор с внутренними нарушителями.

5 Угрозы безопасности информации при разработке программного обеспечения

Номенклатура угроз безопасности информации при разработке ПО, представленная в данном разделе, приведена применительно к процессам жизненного цикла ПО, установленных ГОСТ Р ИСО/МЭК 12207.

5.1 Угрозы безопасности информации при выполнении анализа требований к программному обеспечению

5.1.1 Угроза появления уязвимостей программы вследствие ошибок, допущенных при задании требований по безопасности, предъявляемых к создаваемому программному обеспечению

Данная угроза заключается в преднамеренном или непреднамеренном задании требований по безопасности к создаваемому ПО, содержащих ошибки, которые при условии их необнаружения или неисправления могут стать причиной появления уязвимостей программы. Реализация угрозы может быть связана:

- с преднамеренными действиями нарушителя;
- с принятием разработчиком ПО осознанного решения о неисправлении обнаруженных в требованиях по безопасности ошибок в силу различных причин, например, для сокращения времени разработки программы;
- некачественной или неполной проработкой перечня требований;
- неисправлением обнаруженных ошибок вследствие неосторожных или неквалифицированных действий, неточностями, допущенными в формулировках требований;
- неучетом при формировании требований к разрабатываемому ПО всех применимых источников, например: законов, нормативных правовых актов, отраслевых стандартов, требований пользователя, сценариев применения ПО, актуальных угроз безопасности информации.

Уязвимости программы, появившиеся из-за ошибок в требованиях по безопасности, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на формирование требований по безопасности в процессе их задания или внесения изменений в любые объекты среды разработки ПО, в том числе в элементы конфигурации, создаваемые или используемые при определении этих требований. Изменения могут вноситься путем санкционированного или несанкционированного доступа к объектам среды разработки ПО.

Примечание — В качестве примеров объектов среды разработки ПО можно привести: документы, разрабатываемые по требованиям ГОСТ Р 56939 (техническое задание, задание по безопасности), постановки задач, иные документы, в том числе электронные, создаваемые или используемые при определении требований по безопасности. При выполнении анализа данной угрозы безопасности информации следует учитывать, что объекты среды разработки ПО, создаваемые или используемые при определении требований по безопасности, могут не являться элементами конфигурации, контролируемыми системой управления конфигурацией ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при определении требований по безопасности. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: отсутствием мер, связанных с определением требований по безопасности, неполной или некачественной оценкой сформулированных требований по безопасности, недостатками в мерах, связанных с управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

Примечание — В качестве примеров ошибок в требованиях по безопасности можно привести: ошибки при задании требований к ролям пользователей (отсутствие необходимых ролей, превышение необходимых привилегий и полномочий ролей), отсутствие требования аутентификации для выполнения критичных операций, отсутствие требований по использованию сертифицированных средств криптографической защиты информации.

5.1.2 Угроза выявления уязвимостей программы вследствие раскрытия информации о требованиях по безопасности, предъявляемых к создаваемому программному обеспечению

Данная угроза заключается в преднамеренном или непреднамеренном (из-за неосторожности или неквалифицированных действий работников разработчика ПО) раскрытии информации о требованиях по безопасности, предъявляемых к создаваемому ПО. Нарушение конфиденциальности данной информации может способствовать выявлению недостатков ПО и уязвимостей программы, которые в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем раскрытия информации, содержащейся в объектах среды разработки ПО, в том числе в элементах конфигурации, создаваемых или используемых разработчиком ПО при определении требований по безопасности, вследствие санкционированного или несанкционированного доступа к указанным объектам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при определении требований по безопасности. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО мерах контроля доступа, применяемых к объектам среды разработки ПО и направленных на ограничение круга лиц, имеющих доступ к критичной информации, и операций, которые могут быть выполнены с объектами среды разработки (например, вывод информации с использованием носителей информации или каналов передачи данных);

- недостаточной осведомленностью работников разработчика ПО в области обеспечения конфиденциальности информации.

5.2 Угрозы безопасности информации при выполнении проектирования архитектуры программы

5.2.1 Угроза появления уязвимостей программы вследствие ошибок, допущенных при создании проекта архитектуры программы

Данная угроза заключается в преднамеренном или непреднамеренном создании проекта архитектуры программы (логическая структура программы, в которой идентифицированы компоненты, их интерфейсы и концепция взаимодействия между ними), содержащего ошибки (недостатки), которые при условии их необнаружения или неисправления могут стать причиной появления уязвимостей программы. Реализация угрозы может быть связана:

- с преднамеренными действиями нарушителя;
- с принятием разработчиком ПО осознанного решения о неисправлении обнаруженных в проекте архитектуры программы ошибок в силу различных причин, например для сокращения времени разработки программы,
- с неверной интерпретацией требований по безопасности, предъявляемых к создаваемому ПО, при создании проекта архитектуры программы, неучетом при создании проекта архитектуры программы типовых сценариев компьютерных атак и угроз безопасности информации, неисправлением обнаруженных в проекте архитектуры программы ошибок вследствие случайных неверных или неквалифицированных действий.

Уязвимости программы, появившиеся из-за ошибок в проекте архитектуры программы, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на формирование проекта архитектуры программы, в том числе на моделирование угроз безопасности информации, которые могут возникнуть вследствие применения ПО, или внесения изменений в любые объекты среды разработки ПО, в том числе в элементы конфигурации, создаваемые или используемые при проектировании архитектуры программы. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к объектам среды разработки ПО.

Примечание — В качестве примеров объектов среды разработки можно привести: документы, разрабатываемые по требованиям ГОСТ Р 56939 (результаты моделирования угроз безопасности информации, проект архитектуры программы), постановки задач, иные документы, в том числе электронные, создаваемые или используемые при проектировании архитектуры программы. При выполнении анализа данной угрозы безопасности информации следует учитывать, что объекты среды разработки ПО, создаваемые или используемые при проектировании архитектуры программы, могут не являться элементами конфигурации, контролируемыми системой управления конфигурацией ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при проектировании архитектуры программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: отсутствием мер, связанных с моделированием угроз безопасности информации, которые могут возникнуть вследствие применения ПО, неполным или некачественным моделированием угроз безопасности информации, неучетом результатов моделирования угроз безопасности информации при уточнении проекта архитектуры программы, недостатками в мерах, связанных с управлением конфигурацией ПО, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

Примечание — В качестве примеров ошибок в проекте архитектуры программы можно привести: отсутствие защиты данных, передаваемых между компонентами программы, от раскрытия или модификации, отсутствие проверки входных данных, получаемых из недоверенного источника и передаваемых интерфейсу програм-

мы или интерфейсу компонента программы, отсутствие регистрации событий, критичных с точки зрения защиты информации.

5.2.2 Угроза выявления уязвимостей программы вследствие раскрытия информации о проекте архитектуры программы

Данная угроза заключается в преднамеренном или непреднамеренном (из-за неосторожности или неквалифицированных действий работников разработчика ПО) раскрытии информации, связанной с проектом архитектуры программы. Нарушение конфиденциальности данной информации может способствовать выявлению недостатков ПО и уязвимостей программы, которые в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем раскрытия информации, содержащейся в объектах среды разработки ПО, в том в числе элементах конфигурации, создаваемых или используемых разработчиком ПО при проектировании архитектуры программы, вследствие санкционированного или несанкционированного доступа к указанным объектам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при проектировании архитектуры программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО мерах контроля доступа, применяемых к объектам среды разработки ПО и направленных на ограничение круга лиц, имеющих доступ к критичной информации, и операций, которые могут быть выполнены с объектами среды разработки (например, вывод информации с использованием носителей информации или каналов передачи данных);
- недостаточной осведомленностью работников разработчика ПО в области обеспечения конфиденциальности информации.

5.3 Угрозы безопасности информации при выполнении конструирования и комплексирования программного обеспечения

5.3.1 Угроза внедрения уязвимостей программы в исходный код программы в ходе его разработки

Данная угроза заключается в преднамеренном или непреднамеренном внедрении в исходный код программы ошибок (недостатков), которые при условии их необнаружения или неисправления могут стать причиной появления уязвимостей программы. Реализация угрозы может быть связана:

- с преднамеренными действиями нарушителя;
- с принятием разработчиком ПО осознанного решения о неисправлении обнаруженных в исходном коде программы ошибок в силу различных причин, например для сокращения времени разработки программы;
- с ошибками, внесенными в исходный код программы случайным образом либо вследствие неквалифицированных действий работников, например в случае игнорирования работником правил и рекомендаций, связанных с использованием известных уязвимых конструкций в исходном коде программы.

Уязвимости программы, появившиеся из-за ошибок в исходном коде программы, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем внесения изменений в исходный код программы. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к исходному коду программы.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к исходному коду программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: некачественным или неполным проведением статического анализа или экспертизы исходного кода программы, неучетом при создании программы проекта архитектуры программы и/или порядка оформления исходного кода программы, недостатками в мерах, связанных с управлением конфигурацией ПО, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

Примечание — В качестве примеров преднамеренных ошибок (недостатков) в исходном коде программы, которые могут стать причиной появления уязвимостей программы, можно привести: задание в исходном коде программы аутентификационных данных, внедрение программных закладок. В качестве примеров непреднамеренных ошибок (недостатков) в исходном коде программы, которые могут стать причиной появления уязвимостей программы, можно привести: недостатки, связанные с неконтролируемой форматной строкой, недостатки, связанные с переполнением буфера памяти, недостатки, связанные с неполнотой проверкой вводимых (входных) данных.

5.3.2 Угроза внедрения уязвимостей программы путем использования заимствованных у сторонних разработчиков программного обеспечения уязвимых компонентов

Данная угроза заключается в преднамеренном или непреднамеренном внедрении в разрабатываемую программу заимствованных у сторонних разработчиков ПО компонентов (программные модули, исходный код), содержащих уязвимости. Уязвимости программы, появившиеся из-за применения уязвимых компонентов, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем использования при разработке программных модулей или исходного кода программ сторонних разработчиков, содержащих уязвимости, а также внесения изменений в программные модули или исходный код программ сторонних разработчиков ПО, используемые при разработке программы в среде разработки ПО или в процессе их передачи из среды разработки стороннего разработчика ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к программным модулям или исходному коду программ сторонних разработчиков ПО, используемым при разработке программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: некачественным или неполным анализом уязвимостей в компонентах, заимствованных у сторонних разработчиков ПО, недостатками в мерах, связанных с управлением конфигурацией ПО, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

5.3.3 Угроза внедрения уязвимостей программы из-за неверного использования инструментальных средств при разработке программного обеспечения

Данная угроза заключается в непреднамеренном внесении в программу недостатков из-за ошибок, допущенных при использовании инструментальных средств разработки ПО, или преднамеренной модификации инструментальных средств и объектов среды разработки ПО, содержащих информацию о применяемых при создании программы параметрах инструментальных средств, которые при условии их необнаружения или неисправления могут стать причиной появления уязвимостей программы. Использование в процессе разработки программы модифицированных инструментальных средств, содержащих программные закладки, или неверной информации, связанной с параметрами инструментальных средств, может привести к внедрению в программу уязвимостей. Уязвимости программы, появившиеся из-за ошибок при использовании инструментальных средств или использования модифицированных инструментальных средств или их неверных настроек, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может осуществляться путем:

- использования инструментальных средств способами, не соответствующими порядку их эксплуатации (например, из-за использования ошибочной настройки), вследствие использования инструмен-

тальных средств, применение которых не предусмотрено при разработке ПО, или путем внесения изменений в любые объекты среды разработки ПО, содержащие применяемые при создании программы параметры инструментальных средств;

- модификации или замены инструментальных средств или внесения изменений в любые объекты среды разработки ПО, содержащие информацию о применяемых при создании программы параметрах инструментальных средств.

Изменения могут быть внесены путем санкционированного или несанкционированного доступа к указанным объектам или инструментальным средствам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к инструментальным средствам или объектам среды разработки ПО, содержащим информацию о применяемых при создании программы параметрах инструментальных средств. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: некачественной или неполной идентификацией инструментальных средств разработки ПО и их параметров, недостатками в мерах, связанных с управлением конфигурацией ПО, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

Примечание — К инструментальным средствам относятся, например, трансляторы, компиляторы, редакторы исходного кода программ, отладчики, интегрированные среды разработки.

5.3.4 Угроза появления уязвимостей программы вследствие ошибок, допущенных в эксплуатационных документах в ходе осуществления их разработки и хранения

Данная угроза заключается в преднамеренном или непреднамеренном внесении ошибок в эксплуатационные документы, которые при условии их необнаружения или неисправления могут стать причиной появления уязвимостей программы, связанных с определением ее конфигурации (параметров настройки) и (или) с определением конфигурации ее среды функционирования. Реализация угрозы может быть связана:

- с принятием разработчиком ПО осознанного решения о неисправлении обнаруженных в эксплуатационных документах ошибок в силу различных причин, например, для сокращения времени разработки программы;

- с некорректным, неточным или неполным изложением описания конфигурации (параметров настройки) программы и (или) ее среды функционирования, либо неисправлением обнаруженных ошибок в данных описаниях, вследствие случайных неверных действий или неквалифицированных действий.

Уязвимости программы, связанные с определением ее конфигурации (параметров настройки) и (или) конфигурации ее среды функционирования, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на формирование описаний конфигурации (параметров настройки) программы и (или) ее среды функционирования в процессе разработки эксплуатационных документов или внесения изменений в любые объекты среды разработки ПО, создаваемые или используемые при разработке эксплуатационных документов. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к объектам среды разработки ПО.

Примечание — В качестве примеров объектов среды разработки можно привести: документы, разрабатываемые по требованиям ГОСТ Р 56939 (например, описание применения, руководство оператора), постановки задач, иные документы, в том числе электронные, создаваемые или используемые при разработке эксплуатационных документов. При выполнении анализа данной угрозы безопасности информации следует учитывать, что объекты среды разработки ПО, создаваемые или используемые при разработке эксплуатационных документов, могут не являться элементами конфигурации, контролируемыми системой управления конфигурацией ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при разработке эксплуатационных документов. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разра-

ботки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: в мерах, связанных с управлением конфигурацией ПО, определением в эксплуатационных документах конфигурации (параметров настройки) программы или ее среды функционирования, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

Примечание — В качестве примеров ошибок, которые могут стать причиной появления уязвимостей программы, связанных с определением ее конфигурации (параметров настройки) и (или) с определением конфигурации ее среды функционирования можно привести: ошибки в инструкциях по первоначальной настройке программы (например, отсутствие требования к смене пароля администратора, который был задан разработчиком программы), ошибки в инструкциях по безопасному конфигурированию программы в процессе эксплуатации (например, отсутствие требований о запрете использования словарных паролей), ошибки в инструкциях по безопасному конфигурированию среды функционирования программы (например, отсутствие требования к обязательному применению актуальных обновлений ПО среды функционирования).

5.3.5 Угроза выявления уязвимостей программы вследствие раскрытия исходного кода программы

Данная угроза заключается в преднамеренном или непреднамеренном раскрытии исходного кода программы. Нарушение конфиденциальности данной информации может способствовать выявлению недостатков ПО и уязвимостей программы, которые в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществена путем раскрытия исходного кода программы вследствие санкционированного или несанкционированного доступа.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к исходному коду программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО мерах контроля доступа, применяемых к объектам среды разработки ПО и направленных на ограничение круга лиц, имеющих доступ к критичной информации, и операций, которые могут быть выполнены с объектами среды разработки (например, вывод информации с использованием носителей информации или каналов передачи данных);
- недостаточной осведомленностью работников разработчика ПО в области обеспечения конфиденциальности информации.

5.4 Угрозы безопасности информации при выполнении квалификационного тестирования программного обеспечения

5.4.1 Угроза появления уязвимостей вследствие изменения тестовой документации с целью сокрытия уязвимостей программы

Данная угроза заключается в преднамеренном или непреднамеренном изменении тестовой документации (планы тестирования, описание выполняемых тестов и инструментальных средств, используемых для тестирования программы, фактические результаты тестирования, перечень выявленных при тестировании ПО ошибок ПО и уязвимостей программы), которое может привести к сокрытию информации об уязвимостях программы. Использование модифицированных планов тестирования, описаний выполняемых тестов и описаний ожидаемых результатов тестирования может стать причиной того, что уязвимости программы, внесенные при выполнении анализа требований, проектирования архитектуры программы или конструирования и комплексирования ПО, не будут обнаружены при выполнении квалификационного тестирования ПО. Модификация фактических результатов тестирования или перечня выявленных при тестировании ПО ошибок ПО и уязвимостей программы может стать причиной того, что уязвимости программы, выявленные при тестировании, не будут исправлены. Реализация угрозы может быть связана с принятием разработчиком ПО осознанного решения о невыполнении некоторых тестовых процедур или неисправлении обнаруженных ошибок или уязвимостей программы в силу раз-

личных причин, например, для сокращения времени разработки программы. Уязвимости программы, которые не были обнаружены и (или) исправлены при выполнении тестирования ПО, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на формирование тестовой документации или внесения изменений в любые объекты среды разработки ПО, в том числе в элементы конфигурации, создаваемые или используемые при выполнении тестирования ПО. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к объектам среды разработки ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при выполнении тестирования ПО. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, связанных с управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

5.4.2 Угроза выявления уязвимостей вследствие раскрытия информации о тестировании программного обеспечения

Данная угроза заключается в преднамеренном или непреднамеренном раскрытии информации, связанной с тестированием ПО (планы тестирования, описание выполняемых тестов и инструментальных средств, используемых для тестирования программы, фактические результаты тестирования, перечень выявленных при тестировании ПО уязвимостей программы и ошибок ПО). Нарушение конфиденциальности данной информации может способствовать выявлению недостатков ПО и уязвимостей программы, которые в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем раскрытия информации, содержащейся в объектах среды разработки ПО, в том числе в элементах конфигурации, создаваемых или используемых разработчиком ПО при выполнении тестирования ПО, вследствие санкционированного или несанкционированного доступа к указанным объектам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при выполнении тестирования ПО. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО мерах контроля доступа, применяемых к объектам среды разработки ПО и направленных на ограничение круга лиц, имеющих доступ к критичной информации, и операций, которые могут быть выполнены с объектами среды разработки (например, вывод информации с использованием носителей информации или каналов передачи данных);
- недостаточной осведомленностью работников разработчика ПО в области обеспечения конфиденциальности информации.

5.4.3 Угроза появления уязвимостей программы вследствие совершения ошибок при выполнении тестирования программного обеспечения

Данная угроза заключается в непреднамеренном совершении ошибок при выполнении тестирования ПО. Совершаемые ошибки могут носить случайный характер или быть связаны с неверным выбором стратегий тестирования, недостаточным покрытием тестовыми процедурами проверяемых требований, неточным описанием сценариев тестовых процедур, начальных условий и ожидаемых результатов тестирования, совершением ошибок в процессе выполнения тестирования (воспроизведение начальных условий, реализация тестовых сценариев, использование инструментальных средств способами, не соответствующими порядку их эксплуатации, использование инструментальных средств, применение которых не предусмотрено при тестировании, документирование данного процесса), ошибочной модификацией фактических результатов тестирования ПО или перечня выявленных при тестировании ПО

уязвимостей программы. Уязвимости программы, которые не были обнаружены и (или) исправлены из-за ошибок при выполнении тестирования ПО, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на формирование планов тестирования, ожидаемых или фактических результатов тестирования, перечня выявленных при тестировании ПО уязвимостей программы или внесения изменений в любые объекты среды разработки ПО, в том числе в элементы конфигурации, создаваемые или используемые при выполнении тестирования ПО. При этом изменения вносят путем санкционированного доступа к объектам среды разработки ПО.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах по разработке безопасного ПО, в частности: некачественным или неполным проведением функционального тестирования программы, тестирования на проникновение, динамического анализа кода программы, фаззинг-тестирования программы, недостатками в мерах, связанных с управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

5.5 Угрозы безопасности информации при выполнении инсталляции программы и поддержки приемки программного обеспечения

5.5.1 Угроза внедрения уязвимостей в программу в процессе ее поставки

Данная угроза заключается в преднамеренной несанкционированной модификации программы (дистрибутива программы) в ходе осуществления ее передачи пользователю или непреднамеренной поставке пользователю программы (дистрибутива программы), содержащей известные разработчику ПО уязвимости программы.

Передача пользователю программы, содержащей уязвимости, может быть связана:

- с неверным или неточным описанием процесса поставки ПО пользователю, случайными неверными или неквалифицированными действиями работников при осуществлении передачи ПО пользователю;
- с внедрением в передаваемую программу уязвимостей, а также подмену передаваемой программы на программу, содержащую уязвимости.

Уязвимости программы в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем внесения изменений в программу (дистрибутив программы), которая передается пользователю. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к программе при ее передаче пользователю.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к программе (дистрибутиву программы) при ее поставке пользователю. Реализация данной угрозы внешним нарушителем возможна при условии использования разработчиком ПО для поставки ПО внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО и (или) организацией, привлекаемой разработчиком ПО для поставок ПО (поставщиком ПО), механизмах контроля доступа и контроля целостности, применяемых к передаваемой программе, и мерах по разработке безопасного ПО, в частности: недостатками в процедуре передачи программы пользователю и (или) поставщику ПО, недостатками в мерах, связанных с управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

Примечание — При выполнении анализа данной угрозы безопасности информации в качестве пользователя передаваемой программы (дистрибутива программы) следует рассматривать в том числе сторонние организации, выполняющие интеграцию программы в комплексное изделие информационных технологий, поставляемое пользователям.

5.5.2 Угроза появления уязвимостей программы вследствие модификации эксплуатационных документов при их передаче пользователю

Данная угроза заключается в преднамеренной или непреднамеренной модификации эксплуатационных документов, включая их подмену, с целью внесения в них сведений (некорректных или неточных данных), которые, в случае их необнаружения, могут стать причиной появления уязвимостей про-

граммы, связанных с определением ее конфигурации (параметров настройки) и (или) с определением конфигурации ее среды функционирования. Передача пользователю эксплуатационных документов, содержащих ошибки, может быть связана с неверным или неточным описанием процесса поставки ПО пользователю, случайными неверными или неквалифицированными действиями работников при осуществлении передачи ПО пользователю. Уязвимости программы, связанные с определением ее конфигурации (параметров настройки) и (или) конфигурации ее среды функционирования, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем внесения изменений в эксплуатационные документы, которые передают пользователю. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к эксплуатационным документам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к эксплуатационным документам при их поставке пользователю. Реализация данной угрозы внешним нарушителем возможна при условии использования разработчиком ПО для поставки ПО внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО и (или) организацией, привлекаемой разработчиком ПО для поставок ПО (поставщиком ПО), механизмах контроля доступа и контроля целостности, применяемых к передаваемым эксплуатационным документам, и мерах по разработке безопасного ПО, связанных с возможностью обнаружения пользователем несанкционированных изменений в полученных эксплуатационных документах, управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

5.5.3 Угроза внедрения уязвимостей в обновления программного обеспечения

Данная угроза заключается в получении пользователем обновлений ПО, содержащих внедренные уязвимости программы или уязвимости программы, появившиеся в результате ошибок или неквалифицированных действий работников разработчика ПО при определении и реализации процедуры обновления ПО. Уязвимости программы могут быть внедрены в обновления компонентов ПО собственной разработки, а также в обновления компонентов ПО, которые заимствуют у сторонних разработчиков ПО. Внедрение уязвимостей программы может быть осуществлено путем модификации (включая подмену) обновлений ПО при их передаче пользователю из среды разработки ПО, при их передаче пользователю из среды разработки стороннего разработчика ПО и при их передаче разработчику из среды разработки стороннего разработчика ПО. Уязвимости программы могут быть внедрены в обновления заимствованных у сторонних разработчиков ПО компонентов путем их модификации в среде разработки стороннего разработчика ПО. Внедренные уязвимости программы в дальнейшем могут быть использованы нарушителем с целью выполнения компьютерных атак на информационную систему пользователя.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем внесения изменений в обновления компонентов ПО, а также в обновления компонентов ПО, которые заимствуют у сторонних разработчиков ПО. Изменения могут быть внесены путем санкционированного или несанкционированного доступа к обновлениям ПО.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к обновлениям компонентов ПО, а также к обновлениям компонентов ПО, которые заимствуют у сторонних разработчиков ПО. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО и (или) организацией, привлекаемой разработчиком ПО для поставок ПО (поставщиком ПО), механизмах контроля доступа и контроля целостности, применяемых к обновлениям компонентов ПО собственной разработки, а также к обновлениям компонентов ПО, которые заимствуют у сторонних разработчиков;

- недостатками в процедуре передачи обновлений программы пользователю и (или) поставщику ПО, связанными с отсутствием возможности у пользователя и (или) поставщика ПО обнаружения несанкционированных изменений в полученных обновлениях компонентов ПО собственной разработки, а также в обновлениях компонентов ПО, которые заимствуют у сторонних разработчиков;

- недостатками реализованных разработчиком ПО мерах по разработке безопасного ПО, связанных с проведением систематического поиска уязвимостей программы и обучением работников разработчика ПО в области разработки безопасного ПО.

Примечание — При выполнении анализа данной угрозы безопасности информации в качестве пользователя передаваемого обновления программы следует рассматривать в том числе сторонние организации, выполняющие интеграцию программы в комплексное изделие информационных технологий, поставляемое пользователям.

5.6 Угрозы безопасности информации при решении проблем в программном обеспечении в процессе эксплуатации

5.6.1 Угроза неисправления обнаруженных уязвимостей программы

Данная угроза заключается в том, что обнаруженные ошибки ПО, которые могут стать причиной появления уязвимостей, не исправляют или исправляют несвоевременно вследствие неквалифицированных действий работников разработчика при определении и реализации процедур отслеживания и исправления обнаруженных ошибок ПО.

Обнаруженные ошибки могут быть не исправлены (или несвоевременно исправлены) из-за отсутствия информации, необходимой для устранения, либо по причине того, что информация, необходимая для устранения ошибки, является некорректной. Разработчик в силу различных причин может принять осознанное решение о неисправлении отдельных обнаруженных ошибок, являющихся причиной появления уязвимостей программы, либо отказаться от реализации процедур отслеживания и исправления обнаруженных ошибок программы, принимая последствия негативного влияния такого решения на безопасность разрабатываемого ПО. Причиной отсутствия или некорректности информации, необходимой для устранения ошибок, может являться преднамеренная модификация объектов среды разработки ПО, создаваемых и используемых для определения и реализации процедур отслеживания и исправления обнаруженных ошибок программы. Модификации могут подвергаться как объекты, содержащие информацию, необходимую для устранения ошибок (например, специальная база данных или документально оформленный перечень обнаруженных ошибок), так и инструментальные средства, используемые для реализации процедур отслеживания и устранения обнаруженных ошибок программы, и/или объекты среды разработки ПО, содержащие необходимую информацию о процедурах отслеживания и устранения ошибок ПО или информацию об использовании и параметрах используемых инструментальных средств. Ошибки программы, которые не были исправлены, могут стать причиной уязвимостей передаваемой пользователю программы. Уязвимости программы в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на определение и реализацию процедур отслеживания и исправления обнаруженных ошибок программы или внесения изменений в любые объекты среды разработки ПО, создаваемые или используемые при отслеживании и исправлении обнаруженных ошибок программы, путем осуществления санкционированного или несанкционированного доступа.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым разработчиком ПО при отслеживании и исправлении обнаруженных ошибок программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО механизмах контроля доступа к объектам среды разработки ПО и контроля целостности объектов среды разработки ПО, а также мерах по разработке безопасного ПО, в частности: отсутствием мер, связанных с решением проблем в ПО в процессе эксплуатации, недостатками в процедурах, связанных с отслеживанием и исправлением обнаруженных ошибок ПО и обучением работников разработчика ПО в области разработки безопасного ПО.

5.6.2 Угроза выявления уязвимостей вследствие раскрытия информации об ошибках программного обеспечения и уязвимостях программы

Данная угроза заключается в преднамеренном или непреднамеренном (из-за неосторожности или неквалифицированных действий работников разработчика ПО) раскрытии информации об обнару-

женных ошибках ПО и уязвимостях программы. Нарушение конфиденциальности данной информации может способствовать выявлению уязвимостей программы, которые в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Примечание — В качестве примеров источников информации можно привести: документально оформленный перечень обнаруженных ошибок ПО и уязвимостей программы, базу данных с информацией об обнаруженных ошибках ПО и уязвимостях программы.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем раскрытия информации, содержащейся в объектах среды разработки ПО, в том числе в элементах конфигурации, создаваемых или используемых разработчиком ПО при реализации процедур отслеживания и исправления ошибок, вследствие санкционированного или несанкционированного доступа к указанным объектам.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым при реализации процедур отслеживания и исправления ошибок. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена:

- недостатками в реализованных разработчиком ПО мерах контроля доступа, применяемых к объектам среды разработки ПО и направленных на ограничение круга лиц, имеющих доступ к критичной информации, и операций, которые могут быть выполнены с объектами среды разработки (например, вывод информации с использованием носителей информации или каналов передачи данных);
- недостаточной осведомленностью работников разработчика ПО в области обеспечения конфиденциальности информации.

5.7 Угрозы безопасности информации в процессе менеджмента документацией и конфигурацией программы

В 5.7.1 представлена угроза безопасности информации, связанная с использованием системы управления конфигурацией ПО. Для процесса менеджмента документацией и конфигурацией программы актуальны иные угрозы безопасности информации, связанные с доступом к элементам конфигурации. Эти угрозы безопасности информации представлены в соответствующих пунктахах настоящего стандарта с учетом типа элемента конфигурации следующим образом:

- угроза безопасности информации для элементов конфигурации, связанная с определением требований по безопасности, предъявляемых к создаваемому ПО: 5.1.1;
- угроза безопасности информации для элементов конфигурации, связанная с проектированием архитектуры программы: 5.2.1;
- угроза безопасности информации, связанная с исходным кодом программы: 5.3.1;
- угроза безопасности информации, связанная с программными модулями сторонних разработчиков ПО: 5.3.2;
- угроза безопасности информации, связанная с инструментальными средствами: 5.3.3;
- угрозы безопасности информации, связанные с эксплуатационными документами: 5.3.4, 5.5.2;
- угроза безопасности информации, связанная с тестовой документацией: 5.4.1;
- угроза безопасности информации, связанная с программой (дистрибутивом программы) и обновлениями ПО: 5.5.1;
- угроза безопасности информации, связанная с отслеживанием и исправлением обнаруженных ошибок ПО и уязвимостей программы: 5.6.1.

5.7.1 Угроза внедрения в программу уязвимостей при управлении конфигурацией программного обеспечения

Данная угроза заключается в непреднамеренном совершении ошибок работниками разработчика ПО при управлении конфигурацией ПО или преднамеренной модификации объектов среды разработки ПО, создаваемых или используемых разработчиком ПО при управлении конфигурацией ПО, что может стать причиной появления уязвимостей программы в случае необнаружения модификаций. Совершаемые ошибки могут носить случайный характер или быть связаны с неверным планированием управления конфигурацией ПО, неверной идентификацией элементов конфигурации или эксплуатаци-

ей системы управления конфигурацией ПО способами, не соответствующими порядку ее использования, вследствие случайных неверных или неквалифицированных действий работников разработчика ПО. Совершенные ошибки, при условии их необнаружения или неисправления, могут стать причиной передачи пользователю программы, содержащей известные уязвимости, или эксплуатационных документов, не соответствующих передаваемой программе, что может стать причиной неверной конфигурации программы и (или) ее среды функционирования. Уязвимости программы, появившиеся из-за использования модифицированных объектов среды разработки ПО, создаваемых или используемых разработчиком ПО при управлении конфигурацией ПО, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Примечание — В качестве примера можно привести внесение программных закладок в используемые для управления конфигурацией ПО инструментальные средства, которые будут внедрять уязвимости в создаваемую программу.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на процесс управления конфигурацией ПО или внесения изменений в любые объекты среды разработки ПО, создаваемые или используемые при управлении конфигурацией ПО, путем осуществления санкционированного или несанкционированного доступа.

Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к объектам среды разработки ПО, создаваемым или используемым разработчиком ПО при управлении конфигурацией ПО. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, в частности: в мерах, связанных с управлением конфигурацией ПО, обучением работников разработчика ПО в области разработки безопасного ПО и проведением систематического поиска уязвимостей программы.

Примечание — В качестве примеров объектов среды разработки ПО можно привести: инструментальные средства, используемые для управления конфигурацией ПО, связанную с ними информацию, документы, описывающие использование системы управления конфигурацией ПО.

5.8 Угрозы безопасности информации в процессе менеджмента инфраструктурой среды разработки программного обеспечения

Для процесса менеджмента инфраструктурой среды разработки ПО актуальны угрозы безопасности информации, связанные с доступом к объектам среды разработки, в том числе элементам конфигурации. Эти угрозы безопасности информации представлены в соответствующих пунктах настоящего стандарта с учетом типа объекта среды разработки следующим образом:

- угрозы безопасности информации для элементов конфигурации, связанных с определением требований по безопасности, предъявляемых к создаваемому ПО: 5.1.1, 5.1.2;
- угрозы безопасности информации для элементов конфигурации, связанных с проектированием архитектуры программы: 5.2.1, 5.2.2;
- угрозы безопасности информации, связанные с исходным кодом программы: 5.3.1, 5.3.5;
- угроза безопасности информации, связанная с программными модулями сторонних разработчиков ПО: 5.3.2;
- угроза безопасности информации, связанная с инструментальными средствами: 5.3.3;
- угрозы безопасности информации, связанные с эксплуатационными документами: 5.3.4, 5.5.2;
- угрозы безопасности информации, связанные с тестовой документацией: 5.4.1, 5.4.2;
- угрозы безопасности информации, связанные с программой (дистрибутивом программы) и обновлениями ПО: 5.5.1, 5.5.3;
- угрозы безопасности информации, связанные с отслеживанием и исправлением обнаруженных ошибок ПО и уязвимостей программы: 5.6.1, 5.6.2;
- угрозы безопасности информации, связанные с инструментальными средствами и объектами среды разработки ПО, используемыми для управления конфигурацией ПО: 5.7.1.

При идентификации иных угроз безопасности информации, которые могут возникнуть в процессе менеджмента инфраструктурой среды разработки ПО, разработчик ПО должен руководствоваться положениями ГОСТ Р ИСО/МЭК 27001. При выполнении идентификации активов разработчику ПО следует рассматривать следующие объекты среды разработки ПО и элементы конфигурации:

- программа (дистрибутив программы);
- программные и эксплуатационные документы;
- исходный код программы;
- программные модули, в том числе модули сторонних разработчиков ПО;
- инструментальные средства и связанная с ними информация;
- информация, связанная с обновлениями ПО и устранениями уязвимостей программы;
- перечень выявленных уязвимостей программы.

5.9 Угрозы безопасности информации в процессе менеджмента людскими ресурсами

5.9.1 Угроза появления уязвимостей программы вследствие совершения разработчиком программного обеспечения ошибок при обучении своих работников в области разработки безопасного программного обеспечения

Данная угроза заключается в непреднамеренном совершении ошибок разработчиком ПО при обучении своих работников в области разработки безопасного ПО. Совершаемые ошибки могут носить случайный характер или быть связаны с отсутствием процесса обучения (повышения квалификации) работников, неверным планированием процесса обучения работников или отсутствием пересмотра программ обучения с учетом тенденций в области разработки безопасного ПО. Совершенные ошибки могут стать причиной низкой квалификации работников разработчика ПО в области разработки безопасного ПО. Уязвимости программы, появившиеся из-за низкой квалификации работников разработчика ПО, могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

Реализация данной угрозы внутренним нарушителем может быть осуществлена путем влияния на процесс обучения работников или внесения изменений в любые объекты среды разработки ПО, создаваемые или используемые при их обучении. Изменения при этом вносят путем санкционированного доступа к объектам среды разработки ПО.

Угроза обусловлена недостатками в реализованных разработчиком ПО мерах по разработке безопасного ПО, в частности некачественным обучением работников в области разработки безопасного ПО.

Приложение А
(справочное)

Информация о мерах по разработке безопасного программного обеспечения, установленных ГОСТ Р 56939—2016, реализация которых способствует нейтрализации угроз безопасности информации при разработке программного обеспечения

Таблица А.1 — Соответствие между угрозами безопасности информации при разработке ПО и мерами по разработке безопасного ПО, установленными ГОСТ Р 56939—2016

Угроза безопасности информации при разработке ПО	Мера по разработке безопасного ПО согласно ГОСТ Р 56939—2016
5.1.1 Угроза появления уязвимостей программы вследствие ошибок, допущенных при задании требований по безопасности, предъявляемых к создаваемому программному обеспечению	Определение требований по безопасности, предъявляемых к разрабатываемому ПО (5.1.3.1); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.1.2 Угроза выявления уязвимостей программы вследствие раскрытия информации о требованиях по безопасности, предъявляемых к создаваемому программному обеспечению	Определение, документирование и соблюдение политики информационной безопасности (4.13)
5.2.1 Угроза появления уязвимостей программы вследствие ошибок, допущенных при создании проекта архитектуры программы	Моделирование угроз безопасности информации (5.2.3.1); уточнение проекта архитектуры программы с учетом результатов моделирования угроз безопасности информации (5.2.3.2); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной (4.13); периодический анализ программы обучения работников (5.9.3.2);
5.2.2 Угроза выявления уязвимостей программы вследствие раскрытия информации о проекте архитектуры программы	Определение, документирование и соблюдение политики информационной безопасности (4.13)

Продолжение таблицы А.1

Угроза безопасности информации при разработке ПО	Мера по разработке безопасного ПО согласно ГОСТ Р 56939—2016
5.3.1 Угроза внедрения уязвимостей в исходный код программы в ходе его разработки	Создание программы на основе уточненного проекта архитектуры программы (5.3.3.2); создание (выбор) и использование при создании программы порядка оформления исходного кода программы (5.3.3.3); статический анализ исходного кода программы (5.3.3.4), экспертиза исходного кода программы (5.3.3.5), проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (п. 4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.3.2 Угроза внедрения уязвимостей программы путем использования заимствованных у сторонних разработчиков программного обеспечения уязвимых компонентов	Статический анализ исходного кода программы (5.3.3.4); экспертиза исходного кода программы (5.3.3.5); проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.3.3 Угроза внедрения уязвимостей программы из-за неверного использования инструментальных средств при разработке программного обеспечения	Проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)

Продолжение таблицы А.1

Угроза безопасности информации при разработке ПО	Мера по разработке безопасного ПО согласно ГОСТ Р 56939—2016
5.3.4 Угроза появления уязвимостей программы вследствие ошибок, допущенных в эксплуатационных документах в ходе осуществления их разработки и хранения	Поставка пользователю эксплуатационных документов (5.5.3.2); проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); - защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); - резервное копирование элементов конфигурации (5.8.3.2); - регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3). Определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.3.5 Угроза выявления уязвимостей программы вследствие раскрытия исходного кода программы	Определение, документирование и соблюдение политики информационной безопасности (4.13)
5.4.1 Угроза появления уязвимостей вследствие изменения тестовой документации с целью сокрытия уязвимостей программы	Реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.4.2 Угроза выявления уязвимостей вследствие раскрытия информации о тестировании программного обеспечения	Определение, документирование и соблюдение политики информационной безопасности (4.13)
5.4.3 Угроза появления уязвимостей программы вследствие совершения ошибок при выполнении тестирования программного обеспечения	Функциональное тестирование программы (5.4.3.1), тестирование на проникновение (5.4.3.2), динамический анализ кода программы (5.4.3.3), фаззинг-тестирование программы (5.4.3.4). Реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.5.1 Угроза внедрения уязвимостей в программу в процессе ее поставки	Обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю (5.5.3.1); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1);

Продолжение таблицы А.1

Угроза безопасности информации при разработке ПО	Мера по разработке безопасного ПО согласно ГОСТ Р 56939—2016
5.5.1 Угроза внедрения уязвимостей в программу в процессе ее поставки	использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); - определение, документирование и соблюдение политики информационной безопасности (4.13)
5.5.2 Угроза появления уязвимостей программы вследствие модификации эксплуатационных документов при их передаче пользователю	Обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю (5.5.3.1); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.5.3 Угроза внедрения уязвимостей в обновления программного обеспечения	Обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю (5.5.3.1); проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.6.1 Угроза неисправления обнаруженных уязвимостей программы	Реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)

Окончание таблицы А.1

Угроза безопасности информации при разработке ПО	Мера по разработке безопасного ПО согласно ГОСТ Р 56939—2016
5.6.2 Угроза выявления уязвимостей вследствие раскрытия информации об ошибках программного обеспечения и уязвимостях программы	Определение, документирование и соблюдение политики информационной безопасности (4.13)
5.7.1 Угроза внедрения в программу уязвимостей при управлении конфигурацией программного обеспечения	Проведение систематического поиска уязвимостей программы (5.6.3.4, 5.6.3.5); реализация и использование процедуры уникальной маркировки каждой версии ПО (5.7.3.1); использование системы управления конфигурацией ПО (5.7.3.2—5.7.3.4); защита от несанкционированного доступа к элементам конфигурации (5.8.3.1); резервное копирование элементов конфигурации (5.8.3.2); регистрация событий, связанных с фактами изменения элементов конфигурации (5.8.3.3); определение, документирование и соблюдение политики информационной безопасности (4.13); периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)
5.9.1 Угроза появления уязвимостей программы вследствие совершения разработчиком программного обеспечения ошибок при обучении своих работников в области разработки безопасного программного обеспечения	Периодическое обучение работников (5.9.3.1); периодический анализ программы обучения работников (5.9.3.2)

УДК 004.006.354 ОКС 35.020

Ключевые слова: уязвимость программы, безопасное программное обеспечение, угрозы безопасности информации, защита информации

БЗ 4—2019/13

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 22.05.2018. Подписано в печать 29.05.2018. Формат 60×84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru