УНИВЕРСИТЕТ ИТМО

**А.Н. Бегаев, С.В. Кашин, Н.А. Маркевич,
А.А. Марченко, Д.Д. Павлов**

СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ТРЕБОВАНИЯМ ДОВЕРИЯ

**Санкт-Петербург
2020**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.Н. Бегаев, С.В. Кашин, Н.А. Маркевич, А.А Марченко, Д.Д. Павлов

СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ТРЕБОВАНИЯМ ДОВЕРИЯ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 10.03.01 Информационная безопасность
в качестве учебно-методического пособия для реализации основных
профессиональных образовательных программ высшего образования
бакалавриата

Санкт-Петербург
2020

Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А., Павлов Д.Д., Сертификация программного обеспечения по требованиям доверия – СПб: Университет ИТМО, 2020. – 40 с.

Рецензент(ы):
Заколдаев Данил Анатольевич, кандидат технических наук, доцент, декан факультета безопасности информационных технологий, Университета ИТМО.

Учебно-методическое пособие содержит теоретический и практический материал, посвященный уровням доверия к средствам защиты информации и средствам обеспечения безопасности информационных технологий, а также предъявляемым к ним требованиям.

Содержание

ВВЕДЕНИЕ

Данное учебно-методическое пособие содержит новые материалы, которые позволят студентам получить теоретические знания об уровнях доверия средств технической защиты информации и средств обеспечения безопасности информационных технологий, а также о предъявляемых к ним требованиям в соответствии с Приказом ФСТЭК России №131 от 30.07.2018 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», в ходе изучения дисциплины «Технология сертификации средств защиты информации».

Структурно пособие состоит из семи разделов. Разделы содержат как теоретический, так и практический материал. Практический материал предназначен для подготовки к выполнению лабораторной работы и получения знаний в части моделирования угроз информационной безопасности в программном обеспечении по методу STRIDE. Пособие содержит лабораторную работу и контрольные вопросы, призванные помочь студентам в освоении результатов обучения по дисциплине «Технология сертификации средств защиты информации».

Дополнительно приведен библиографический список (список рекомендуемой литературы), который включает руководящие документы и литературу, рекомендуемую авторами для более глубокого освоения содержания дисциплины.

1 ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии с Федеральным законом № 184 «О техническом регулировании» сертификация представляет собой форму осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров.

Сертификация может быть обязательной и добровольной. Обязательная сертификация осуществляется на основании законов и законодательных положений и проводится в системах обязательной сертификации, например, в системе сертификации средств защиты информации, которая регламентируется Постановлением Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». Добровольная сертификация проводится только по инициативе заявителя (юридического или физического лица) в системах добровольной сертификации.

В соответствии с Постановлением Правительства № 608 обязательная сертификация проводится в рамках систем сертификации Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства обороны Российской Федерации (Минобороны России).

Система сертификации ФСТЭК России – это структура, состоящая из следующих участников сертификации:

- федерального органа по сертификации (ФСТЭК России);
- организаций, аккредитованных ФСТЭК России в качестве органов по сертификации (органы по сертификации);
- организаций, аккредитованных ФСТЭК России в качестве испытательных лабораторий (испытательные лаборатории);
- изготовителей (производителей) средств защиты информации.

Сертификация в системе ФСТЭК России проводится в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 года № 55.

Сертификация средств защиты информации осуществляется на соответствие нормативным правовым актам ФСТЭК России, техническим условиями (ГОСТ 2.114-2016), техническим заданиям (ГОСТ 19.201-78), заданиям по безопасности (ГОСТ Р ИСО/МЭК 15408).

С 1 июня 2019 г. при обязательной сертификации средств защиты информации оценка доверия не проводится по ГОСТ Р ИСО/МЭК 15408-3-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности» от 01.09.2014 в связи с утверждением приказа ФСТЭК

России № 131 от 30 июля 2018 года «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

1.1 Общие требования ГОСТ Р ИСО/МЭК 15408-3

Данный документ определяет требования доверия и включает оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия для компонентов средств, составные пакеты доверия, определяющие шкалу для измерения доверия для составных средств, отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии для оценки профилей защиты и заданий по безопасности.

Оценка является традиционным способом достижения доверия, и она положена в основу ИСО/МЭК 15408. Методы оценки могут, в частности, включать в себя:

- анализ и проверку процессов и/или процедур;
- проверку того, что процессы и/или процедуры действительно применяются;
- анализ соответствия между представлениями проекта средства;
- верификацию доказательств;
- анализ соответствия каждого представления проекта средства требованиям;
- анализ руководств;
- анализ разработанных функциональных тестов и предоставленных результатов;
- независимое функциональное тестирование;
- анализ уязвимостей, включающий предположения о недостатках;
- тестирование на проникновение.

В ИСО/МЭК 15408 определены семь иерархически упорядоченных оценочных уровней доверия для оценки уровня доверия к средствам. Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т. е. увеличением строгости, области охвата и/или глубины оценки) и добавлением компонентов из других семейств доверия (т. е. добавлением новых требований).

Оценочные уровни доверия включались в профили защиты средств защиты информации (межсетевых экранов, систем обнаружения вторжений, средств антивирусной защиты и т. п.). С введением в действие

Приказа ФСТЭК №131 применение оценочных уровней доверия при формировании требований к средствам защиты было остановлено.

1.2 Общие требования Приказа ФСТЭК №131

В соответствии с Приказом ФСТЭК №131 для разграничения требований по безопасности информации к программным, программно-техническим средствам технической защиты информации, средствам обеспечения безопасности информационных технологий, включая защищенные средства обработки информации (далее – средства), устанавливается 6 уровней доверия.

Каждое средство, соответствующие определенному уровню, может применяться в 5 различных системах определенного класса. Это соответствие отражено в таблице 1.

Таблица 1 – Общие требования уровней доверия

	6 УД	**5 УД**	**4 УД**	**3 УД**	**2 УД**	**1 УД**
КИИ[1]	3 категория	2 категория	1 категория	Применяются для защиты сведений, составляющих государственную тайну		
ГИС[2]	3 класс	2 класс	1 класс			
АСУ ТП[3]	3 класс	2 класс	1 класс			
ИСПДн[4]	3, 4 уровень	2 уровень	1 уровень			
ИСОП[5]			II класс			

Выполнение Требований к уровню доверия является обязательным при проведении работ по сертификации средств защиты информации, организуемых ФСТЭК России в пределах своих полномочий.

Средства защиты информации, соответствующие 6 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных.

---

[1] КИИ (сокр. – критическая информационная инфраструктура). Категории устанавливаются в соответствии с Федеральным законом № 187-ФЗ от 26.07.2017 и Постановлением Правительства РФ № 127 от 08.02.2018.

[2] ГИС (сокр. – государственная информационная система). Классы устанавливаются в соответствии с Приказами ФСТЭК России № 17 от 11.02.2013 и № 27 от 15.02.2017.

[3] АСУ ТП (сокр. – автоматизированная система управления технологическим процессом). Классы устанавливаются в соответствии с Приказами ФСТЭК России № 31 от 14.03.2014 и № 138 от 09.08.2018.

[4] ИСПДн (сокр. – информационная система персональных данных). Уровни защищенности устанавливаются в соответствии с Постановлением Правительства № 1119 от 01.11.2012.

[5] ИСОП (сокр. – информационная система общего пользования). Классы устанавливаются в соответствии с Приказом ФСБ России и ФСТЭК России № 416/489 от 31.08.2010.

Средства защиты информации, соответствующие 5 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 2 категории, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Средства защиты информации, соответствующие 4 уровню доверия, подлежат применению в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

Средства защиты информации, соответствующие 1, 2 и 3 уровням доверия, применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Если описывать требования 131 Приказа на «языке» ИСО/МЭК 15408, то установлено 3 класса требований, каждый из который состоит из определенного количества подклассов (семейств). А компонент доверия как элемент оценки уровня доверия не используется в явном виде (нет привязки конкретного требования к компоненту).

В таблице 2 представлено сравнение двух документов.

Таблица 2 – Сравнение Приказа №131 и ГОСТ Р ИСО/МЭК 15408-3

ГОСТ Р ИСО/МЭК 15408-3	**Приказ ФСТЭК №131**
Уровни доверия	
7 уровней	6 уровней
Требования	
Разработка (6 семейств)	Разработка (10 подпунктов)
Руководства (2 семейства)	
Тестирование (4 семейства)	Испытания (3 подпункта)
Оценка уязвимостей (1 семейство)	
Поддержка жизненного цикла (7 семейств)	Поддержка безопасности (3 подпункта)
Оценка задания по безопасности (7 семейств)	–

2 ТРЕБОВАНИЯ К РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВА

При разработке и производстве средства необходимо выполнить мероприятия, предусматривающие:

- разработку модели безопасности средства;
- проектирование архитектуры безопасности средства;
- разработку функциональной спецификации средства;
- проектирование средства;
- разработку представления реализации средства;
- выбор средств, применяемых при разработке средства;
- управление конфигурацией средства;
- разработку документации по безопасной разработке средства[6];
- разработку руководства пользователя средства;
- разработку руководства администратора средства.

Средство соответствует уровню доверия, если оно удовлетворяет соответствующим требованиям к разработке и производству средства, приведенным в таблице 3.

Таблица 3 – Требования к разработке

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1	Требования к разработке и производству средства:			
1.1	требования к разработке модели безопасности средства			+
1.2	требования к проектированию архитектуры безопасности средства	+	=	=
1.3	требования к разработке функциональной спецификации средства	+	+	+
1.4	требования к проектированию средства	+	=	=
1.5	требования к разработке представления реализации средства	+	+	+
1.6	требования к средствам, применяемым для разработки средства	+	=	=
1.7	требования к управлению конфигурацией средства	+	+	+
1.8	требования к разработке документации по безопасной разработке средства	+	=	=

[6] ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» от 01.06.2017.

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1.9	требования к разработке руководства пользователя средства	+	=	=
1.10	требования к разработке руководства администратора средства	+	=	=

Обозначение «+» в строке требования к уровню доверия указывает на наличие требований, предъявляемых к соответствующему уровню доверия.

Обозначение «=» означает, что требования к уровню доверия соответствуют требованиям, предъявляемым к предыдущему уровню доверия.

2.1 Требование к разработке модели безопасности средства

Модель безопасности представляет собой формальное (математическое) описание условий безопасности. Такое описание позволяет провести независимую от разработчика модели проверку ее корректности. Чаще всего для этих целей модели формируются в виде набора булевых утверждений, которые автоматически доказываются при помощи специальных инструментов – SAT и SMT решателей.

Модель безопасности на средство защиты должно разрабатываться начиная с 4 уровня доверия. Для подтверждения соответствия 4 уровню доверия необходимо описать правила разграничения и управления доступом к средству, правила фильтрации информационных потоков и описать так называемые «условия безопасности», т. е. формально доказать, что модель безопасности средства реализует правила (политики) безопасности.

Более подробно про верификацию политик безопасности на примере операционной системы Astra Linux можно узнать из монографии «Моделирование и верификация политик безопасности управления доступом в операционных системах» П.Н. Девянина, Д.В. Ефремова, В.В. Кулямина и др.[7]

[7] Моделирование и верификация политик безопасности управления доступом в операционных системах / П. Н. Девянин, Д. В.Ефремов, В. В.Кулямин и др. – М.: Горячая линия – Телеком, 2019. – 214 с.: ил. ISBN 978-5-9912-0787-4

2.2 Требования к проектированию архитектуры безопасности средства

Для уровней доверия, относящимся к средствам, не использующимся в системах обработки информации, содержащей государственную тайну, спроектированная архитектура безопасности средства должна обеспечивать:

– невозможность получения несанкционированного доступа к средству посредством обхода реализуемых функций безопасности;

– защиту функций безопасности средства.

2.3 Требования к разработке функциональной спецификации

Данные требования содержат дополнения на каждом последующем уровне доверия (для выполнения требований определенного уровня необходимо учитывать совокупность указаний предыдущих уровней и дополнений текущего).

Так, для 6 уровня доверия функциональная спецификация средства должна описывать функции безопасности средства и должна быть полным и точным отображением функциональных требований безопасности. Также, она должна включать:

– детализированное описание интерфейсов функций безопасности, через которые пользователь взаимодействует с этими функциями;

– определение интерфейсов, не влияющих на функции безопасности средства.

Для 5 уровня доверия функциональная спецификация должна содержать описание назначения и методов использования всех интерфейсов функций безопасности, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

Для выполнения требования по 4 уровню доверия функциональная спецификация должна предусматривать описание действий со всеми интерфейсами функций безопасности, не влияющим на выполнение функциональных требований, обеспечивая, где это необходимо, детализацию результатов и сообщений об ошибках.

2.4 Требования к проектированию средства

Требования применимы в равной мере как для 6, так и для 5 и 4 уровней доверия, и содержат следующие пункты:

– проектирование средства должно включать в себя определение списка подсистем (с входящими в их состав модулями): реализующих функции безопасности средства, поддерживающих выполнение функций безопасности, не влияющих на выполнение функций безопасности;

– документация должна включать: описание структуры средства и всех ее подсистем, описание взаимодействия подсистем средства между собой, описание всех модулей средства.

2.5 Требования к разработке представления реализации средства

Для соответствия 6 уровню доверия необходимо, чтобы представление реализации содержало (для аппаратной платформы программно-технического средства) перечень аппаратных устройств (микросхем), которые влияют на функции безопасности. Также на средство необходимо разработать формуляр, который должен содержать контрольные суммы дистрибутива и исполняемых файлов программного обеспечения средства. Контрольные суммы должны уточняться при обновлении средства.

Для 5 уровня доверия необходимо предоставить в испытательную лабораторию все структурные схемы и техническую документацию на аппаратные средства (при наличии), а для программного обеспечения – исходные тексты ПО, с указанием значений контрольных сумм файлов.

Для 4 уровня доверия представление реализации фиксирует детализированное внутренние содержание функций безопасности на уровне исходного текста, аппаратных схем и т. п.

2.6 Требования к средствам, применяемым для разработки средства

Для всех уровней доверия должна быть разработана документация, включающая описания средств, применяемых для разработки программного, программно-технического средства технической защиты информации, средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации, с учетом использованных конфигураций. К таким средствам обычно относятся компиляторы, отладчики, среды разработки, инструментальные средства тестирования.

Чтобы понять глубину необходимого описания средств, применяемых при разработки, можно воспользоваться ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее – ГОСТ Р 56939-2016). Так, ГОСТ Р 56939-2016 предписывает идентифицировать инструментальные средства разработки и документировать для них:

– наименование и идентификационные признаки;
– наименование разработчиков средств;
– ссылки на эксплуатационные документы;

– значения настроек, применяемых при создании программы.

Пример идентификации компилятора

Наименование	Clang 8
Разработчик	LLVM Project
Документация	https://releases.llvm.org/8.0.0/tools/clang/docs/index.html
Настройки	D_FORTIFY_SOURCE=2, W1, O2, fstack-protector-all, fsanitize=safe-stack.

Документирование настроек компилятора очень важно с точки зрения генерации одинакового исполняемого кода разными разработчиками. Некоторые настройки компилятора, например, уровень оптимизации, могут вносить или удалять части инструкций из исполняемого кода.

Аналогичное документирование следует проводить и для иных средств разработки. Так, следует документировать и довести до сведения разработчиков настройки среды разработки, включая выбранный стиль написания кода – это позволит сократить время на экспертизу кода.

2.7 Требования к управлению конфигурацией средства

Для 6 уровня доверия управление конфигурацией средства должно контролировать изменения средства и документацию на него, а также, обеспечивать его уникальную маркировку.

Документация должна включать все вышеперечисленные функции системы управления конфигурацией и список элементов, входящий в состав системы.

Для 5 уровня доверия дополнительно должны контролироваться изменения составных частей средства и обеспечиваться уникальная идентификацией всех элементов конфигурации.

Документация должна включать описание метода, используемого для уникальной идентификации элементов конфигурации (с указанием автора для каждого элемента).

Для 4 уровня доверия должно предусматриваться:

– применение автоматизированных мер контроля, обеспечивающих внесение в элементы конфигурации только санкционированных изменений;

– методы учета модифицированных или вновь созданных элементов конфигурации.

Для контроля изменений исходного кода и документации рекомендуется использовать специализированное программное обеспечение – системы контроля версии такие, как git, SVN, Mercurial.

Порядок работы в системе контроля версий должен быть задокументирован. Права на работу в системе должны выдаваться соответствующим образом, чтобы избежать попадания неавторизованного кода в основную ветку репозитория программного средства.

2.8 Требования к разработке документации по безопасной разработке средства

Для каждого уровня доверия на средство должна быть разработана документация по безопасности разработки средства, которая должна включать описание мер для обеспечения конфиденциальности и целостности документации на средство и самого средства, а также мер, направленных на снижение вероятности возникновения уязвимостей и слабостей в средстве. Из ГОСТ Р 56939-2016 можно выделить 7 групп мер, которые необходимо применять.

Группа 1. Меры при проектировании архитектуры

При проектировании архитектуры следует в первую очередь определить требования по безопасности, предъявляемые к разрабатываемому средству и задокументировать его проект архитектуры. На основании проекта архитектуры производится моделирование угроз безопасности, которые могут возникнуть вследствие применения средства. Методология моделирования угроз должна быть задокументирована. По результатам моделирования угроз оформляется список выявленных угроз и принимаются проектные решения и указания разработчикам для их нейтрализации. При применении ГОСТ Р 56939-2016 и внедрении мер, в частности, при моделировании угроз безопасности, стоит обращаться к ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения».

Группа 2. Меры при конструировании и комплексировании средства

На этапе конструирования и комплексирования средства, то есть в процессе написания исходного кода по проекту архитектуры и сборке исполняемого кода, необходимо, в первую очередь, внедрить меры, которые гарантировали бы использование командой программистов только идентифицированных средств разработки. Также на этом этапе проводится статический анализ исходного кода и происходит доработка программы по его результатам.

Группа 3. Меры при квалификационном тестировании средства

Квалификационное тестирование включает в себя функциональное тестирование, тестирование на проникновение, динамический анализ и фаззинг-тестирование.

Функциональное тестирование – тестирование заявленного в документации функционала средства и выявление отличий между его требуемыми свойствами и обнаруживаемыми.

Тестирование на проникновение – метод выявления слабостей и уязвимостей в продукте, имитирующий действия потенциального нарушителя. Тестирование на проникновение подразумевает, что потенциальный нарушитель не обладает доступом к исходным текстам продукта, т. е. действует по методу «черного ящика». Однако, даже исходя из архитектуры и свойств продукта, можно понять, какие возможные ошибки могут в нем содержаться.

Пример

Средство защиты управляется администратором через веб-браузер. Значит, средство может содержать ошибки, характерные для продуктов, в который применяются веб-технологии и базы данных. Например, межсайтовая подделка запроса, межсайтовый скриптинг, подделка запросов со стороны сервера, SQL-инъекции.

Понять, как подтвердить наличие предполагаемых в средстве ошибок, поможет база CAPEC[8]. Это база знаний, которая содержит 517 шаблонов атак и действий злоумышленников, которые структурированы и категорированы по механизмам и своей направленности.

Полное представление шаблона атаки состоит из:

- описания атаки;
- вероятности атаки;
- тяжести атаки;
- связи с другими шаблонами классификации CAPEC;
- пошаговой инструкции совершения атаки;
- предпосылок к атаке;
- требуемых навыков злоумышленника;
- требуемых ресурсов;
- последствий;
- противодействий;
- примеров;
- релевантных слабостей программного обеспечения по классификации CWE.

[8] Common Attack Pattern Enumeration and Classification (CAPEC) – https://capec.mitre.org/

Пример. Инъекция аргументов

<table>
<tr><td colspan="2" rowspan="2">CAPEC-6</td><td>Вероятность</td><td>Тяжесть</td><td>Класс</td><td>Область</td><td>Механизм</td></tr>
<tr><td>Высокая</td><td>Высокая</td><td>Инъекции</td><td>ПО</td><td>Инъекция</td></tr>
<tr><td colspan="7">Злоумышленник изменяет поведение приложения путем подачи данных или команд в функции приложения, которые не фильтруют или не санитизируют входные данные</td></tr>
<tr><td colspan="7">HOWTO</td></tr>
<tr><td rowspan="2">Подготовка</td><td colspan="6">Определение потенциального вектора атаки
Используя автоматическое средство или действуя вручную, злоумышленник идентифицирует службы или методы, которые потенциально могут использоваться в качестве векторов внедрения (ОС, API, процедуры SQL и т. д.).</td></tr>
<tr><td colspan="6">Техники
Исследуйте приложение вручную и запишите все возможные места, куда могут быть переданы аргументы.
Используйте парсеры веб-приложений, чтобы создать взаимосвязь между URL-ами и входными данными на странице.</td></tr>
<tr><td rowspan="2">Эксперимент</td><td colspan="6">Попытка изменения аргументов
Возможно, с использованием инструментария, злоумышленник выполнит инъекцию различных вариантов аргументов.</td></tr>
<tr><td colspan="6">Техники
Постарайтесь использовать как можно больше вариантов проверок на уязвимость внедрения аргументов, фиксируя при этом положительный результат и тип атакуемой системы.
Используйте инструменты для ведения логов, записи результатов и сообщений об ошибках, если это возможно.</td></tr>
<tr><td rowspan="2">Эксплуатация</td><td colspan="6">Взлом приложения
Злоумышленник, используя определенный синтаксис, вводит инъекции аргументов, что создает вредоносный эффект в целевом приложении.</td></tr>
<tr><td colspan="6">Техники
Ручной ввод полезной нагрузки в конкретное уязвимое место</td></tr>
<tr><td colspan="7">Предпосылки</td></tr>
<tr><td colspan="7">ПО не способно отфильтровать входные данные, которые поступают от пользователя.
ПО разрешает выполнение неотфильтрованных или неподтвержденных входных данных в оболочке ОС, и, при необходимости, конфигурация системы позволяет отправлять выходные данные обратно</td></tr>
<tr><td colspan="2">Навыки</td><td colspan="2">Средние</td><td colspan="3">Ресурсы</td></tr>
<tr><td colspan="3">Злоумышленник должен определить вектор внедрения, идентифицировать команды, специфичные для ОС и, при необходимости, собрать выходные данные</td><td colspan="4">Возможность синхронного/асинхронного взаимодействия с сервером. Опционально – возможность захвата вывода</td></tr>
<tr><td colspan="7">Последствия</td></tr>
<tr><td colspan="5">Конфиденциальность, управление доступом, авторизация</td><td colspan="2">Повышение привилегий</td></tr>
<tr><td colspan="5">Целостность</td><td colspan="2">Изменение данных</td></tr>
<tr><td colspan="5">Конфиденциальность</td><td colspan="2">Чтение данных</td></tr>
</table>

Противодействие	
Проектирование	Не позволяйте пользователю передавать аргументы в оболочку ОС до тех пор, пока он не авторизован. Создайте функцию, которая будет преобразовывать и санитизировать пользовательский ввод. Ограничьте привилегии для ПО. Даже если пользователь получит доступ к оболочке, код будет выполнен не от имени привилегированной учетной записи.
Реализация	Реализуйте в ПО журнал аудита с возможностью отправки на удаленный хост. Это поможет в случае компрометации собрать доказательства и подробности инцидента.

CWE ref.	
CWE-ID	**Название слабости**
74	Некорректная нейтрализация специальных элементов в выходных данных, используемых нижележащим компонентов («Инъекция»)
146	Некорректная нейтрализация разделителей команд/выражений
184	Неполный черный список
78	Некорректная нейтрализация специальных элементов, используемых в построении команды ОС («Инъекция команды ОС»)
185	Некорректное регулярное выражение
697	Некорректное сравнение

Динамический анализ – анализ программы в режиме ее непосредственного выполнения. Динамический анализ чаще всего не задействует исходные тексты программы, однако возможны и случаи, при которых исходные тексты модифицируются специальными командами (инструментируются), что позволит повысить точность динамического анализа. Популярными средствами анализа из этого семейства являются:

– Valgrind[9] – не просто готовый инструмент динамического анализа, а скорее фреймворк для создания своих собственных;

– angr[10] – платформо-независимый фреймворк для анализа бинарных файлов;

– Java PathFinder[11] – model checking инструмент для Java байт-кода.

Фаззинг-тестирование – передача программе случайных или специально сформированных данных с последующей оценкой ее свойств. Фаззинг позволяет найти ошибки, связанные с некорректной обработкой пользовательского ввода и работой с памятью.

[9] Valgrind – http://valgrind.org/
[10] angr – https://github.com/angr/angr
[11] Java PathFinder – https://github.com/javapathfinder/jpf-core

Группа 4. Меры при инсталляции и поддержке приемки средства

На этапе инсталляции пользователь должен иметь возможность удостовериться, что полученное им ПО не было скомпрометировано. Это достигается разработчиком путем расчета эталонных контрольных сумм дистрибутива ПО и внесения полученных значений в эксплуатационную документацию (в формуляр).

Группа 5. Меры при решении проблем в средстве в процессе эксплуатации

Слабости и уязвимости ПО выявляются не только при его направленном тестировании, но и при эксплуатации пользователем. Разработчик должен внедрить процедуры отслеживания и исправления обнаруженных ошибок и уязвимостей ПО, а также проводить систематический поиск уязвимостей программы.

Поиск уязвимостей представляет собой прохождение всех этапов из групп 1-4. Так, если после релиза в ПО были внесены изменения, эти изменения должны согласовываться с проектом архитектуры, для изменений должны быть смоделированы угрозы и изменение должно пройти все этапы квалификационного тестирования.

Группа 6. Меры в процессе менеджмента документации, конфигурации и инфраструктуры среды разработки средства

Реализация группы мер заключается во внедрении уникальной маркировки версий ПО и использовании системы управления конфигурации ПО, по-другому – системы контроля версий.

Все изменения, вносимые в инфраструктуру среды разработки, должны быть контролируемы. Хорошей практикой является применение формализованной политики изменений, которая позволила бы отслеживать изменения, проводить оценку их эффективности и, в случае неудачи, давала бы возможность вернуться к прежнему состоянию.

Инфраструктура среды разработки должна быть защищена от несанкционированного доступа. Для этих целей рекомендуется внедрить резервное копирование элементов конфигурации, а также регистрацию событий.

Группа 7. Меры в процессе менеджмента людскими ресурсами.

Разработчики должны проходить обучение в области безопасной разработки. Обучение может быть как внутренним, так и с привлечением сторонних организаций.

2.9 Требования к разработке руководства пользователя средства

Для всех уровней доверия на средство должно быть разработано руководство пользователя средства с описанием:

– режимов работы средства;
– принципов безопасной работы средства;
– функций и интерфейсов функций средства, доступных каждой роли пользователей;
– параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений;
– типов событий безопасности, связанных с доступными пользователю функциями средства;
– действий после сбоев и ошибок эксплуатации средства.

2.10 Требования к разработке руководства администратора средства

Для каждого уровня доверия на средство должно быть разработано руководство администратора средства с описанием:
– действий по приемке поставленного средства;
– действий по безопасной установке и настройке средства;
– действий по реализации функций безопасности среды функционирования средства.

3 ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ИСПЫТАНИЙ СРЕДСТВА

При проведении сертификации средства защиты информации испытательная лаборатория должна провести испытания, которые предусматривают:

– тестирование средства;

– испытания по выявлению уязвимостей и недекларированных возможностей средства[12];

– проведение анализа скрытых каналов в средстве.

Средство соответствует уровню доверия, если оно удовлетворяет соответствующим требованиям к проведению испытаний средства.

Таблица 4 – Требования к проведению испытаний

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
2	Требования к проведению испытаний средства:			
2.1	требования к тестированию средства	+	+	+
2.2	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	+	+	+
2.3	требования к проведению анализа скрытых каналов в средстве		+	=

Обозначение «+» в строке требования к уровню доверия указывает на наличие требований, предъявляемых к соответствующему уровню доверия.

Обозначение «=» означает, что требования к уровню доверия соответствуют требованиям, предъявляемым к предыдущему уровню доверия.

3.1 Требования к тестированию средства

Для 6 уровня доверия средство должно быть протестировано. Тестовая документация должна включать:

– сведения о периодичности проведения тестирования на проникновение, план тестирования, описание выполняемых тестов и инструментальных средств;

[12] «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении», утвержденная ФСТЭК России от 01.06.2019

– сценарий проведения тестов, учитывая зависимость последовательности выполнения одних тестов от результатов других;

– описание ожидаемых результатов тестирования;

– описание фактических результатов тестирования, их сопоставление с ожидаемыми результатами тестирования и на его основе – выводы.

Для 5 уровня доверия тестовая документация должна включать описание сопоставления тестов с подсистемами средства, показывая тем самым, что тесты охватывают всю систему в общем.

При проведении тестирования средства проводится оценка влияния на подсистемы средства, реализующие функции безопасности, других подсистем средства.

Для 4 уровня доверия тестовая документация должна включать описание сопоставления тестов с составляющими подсистем – модулями. И так же, как и для 5 уровня, необходимо провести оценку влияния на модули, реализующие функции безопасности, других модулей средства.

3.2 Требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства

Для 6 уровня доверия должны быть проведены испытания по выявлению уязвимостей и недекларированных возможностей по 6 уровню контроля.

Для 5 уровня доверия должны быть проведены испытания по 5 уровню контроля.

Для 4 уровня доверия должны быть проведены испытания по 4 уровню контроля.

3.3 Требования к проведению анализа скрытых каналов в средстве

Для 6 уровня данные требования не предъявляются.

Для 4 и 5 уровней доверия в средстве должны быть проведены определение и анализ скрытых каналов по памяти. То есть, найдены и проанализированы участки памяти, в которые записывается защищаемая информация и которые не учитываются разработчиками системы защиты и не выявляются применяемыми средствами защиты информации.

В итоге необходимо разработать требования для среды функционирования средства с целью ограничения, слежения, полного или частичного устранения выявленных скрытых каналов, которые могут привести к утечке информации секретного характера.

Вся используемая и полученная информация должна быть отражена в соответствующей документации.

4 ТРЕБОВАНИЯ К ПОДДЕРЖКЕ БЕЗОПАСНОСТИ СРЕДСТВА

Средство должно обеспечиваться поддержкой безопасности, предусматривающей:

– устранение недостатков средства;

– обновление средства;

– документирование процедур устранения недостатков и обновление средства.

Средство соответствует уровню доверия, если оно удовлетворяет соответствующим требованиям к поддержке безопасности средства.

Таблица 5 – Требования к поддержке безопасности

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
3	Требования к поддержке безопасности средства:			
3.1	требования к устранению недостатков средства	+	+	+
3.2	требования к обновлению средства	+	+	+
3.3	требования к документированию процедур устранения недостатков и обновления средства	+	=	=

Обозначение «+» в строке требования к уровню доверия указывает на наличие требований, предъявляемых к соответствующему уровню доверия.

Обозначение «=» означает, что требования к уровню доверия соответствуют требованиям, предъявляемым к предыдущему уровню доверия.

4.1 Требования к устранению недостатков средства

Для 6 уровня доверия предъявляются следующие требования:

– поиск в открытых источниках информации о недостатках средства или недостатках в модулях, производимых другими разработчиками;

– получение сведений о недостатках средства от пользователей средства;

– проведение испытаний средства по выявлению недостатков в средстве, в том числе по выявлению уязвимостей и недекларированных

возможностей средства (а также, проведение испытаний после доработки средства для подтверждения устранения уязвимостей);

– устранение недостатков средства путем доработки средства или его отдельных компонентов; разработку альтернативных мер по защите информации или ограничений по применению средства, снижающих возможность эксплуатации уязвимостей;

– доведение информации о недостатках средства, а также об альтернативных мерах или ограничений по применению до потребителей, ФСТЭК России и банка данных угроз безопасности информации;

Для 5 уровня доверия дополнительно предъявляются следующие требования:

– разработка альтернативных мер по защите информации или ограничений по применению средства, а также доведение информации о недостатках и указанных мерах и ограничениях до потребителей должны осуществляться в установленные сроки;

– доработка средства, в том числе разработка обновлений программного обеспечения средства, или разработка мер по защите информации, нейтрализующих недостаток, должна осуществляться в срок не более 2 месяцев с момента выявления недостатка.

Для 4 уровня доверия:

– доведение информации должно осуществляться до каждого потребителя путем отправки сообщений на электронные адреса или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

4.2 Требования к обновлению средства

Для 6 уровня доверия предъявляются следующие требования:

– информирование потребителей средства о выпуске обновлений;

– обеспечение возможности получения обновления средства способами, обеспечивающими его целостность.

Для 5 уровня доверия дополнительно предъявляются следующие требования:

– все обновления средства должны поступать на средство с сервера разработчика;

– при доведении обновлений средства до потребителей должны обеспечиваться подлинность и целостность обновлений за счет применения электронной подписи.

Для 4 уровня доверия выдвинуты следующие требования:

– доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя индивидуально посредством

отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

4.3 Требования к документированию процедур устранения недостатков и обновления средства

Для всех уровней доверия предъявляются следующие требования:

– включение в программную и конструкторскую документацию на средство процедур устранения недостатков;

– разработку регламента обновления средства потребителем, включающего порядок получения, установки и контроля установки обновления программного обеспечения средства.

Об окончании производства и/или поддержки безопасности средства необходимо проинформировать потребителей и ФСТЭК России не позднее чем за 12 месяцев до окончания обслуживания средства.

5 МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВОЗНИКАЮЩИХ ПРИ ЕГО ПРИМЕНЕНИИ

Как было сказано ранее, на основе проекта архитектуры программы разработчик проводит моделирование угроз безопасности информации программного обеспечения, которые возникают при его применении. Существует множество методологий моделирования таких угроз, самой зрелой из которых признана STRIDE[13].

Методология STRIDE была разработана в Microsoft в 1999 году (сотрудниками Loren Kohnfelder и Praerit Garg) и изначально была лишь документом для внутреннего использования. В то время многие в Microsoft называли ее «Угрозой нашему программному обеспечению»[14]. Видимо, разработчики были не рады тому, что на их плечи ложилась дополнительная работа по построению моделей угроз.

Название этой модели является аббревиатурой от шести основных типов угроз:

- **S**poofing (англ. Спуфинг – Подмена).
- **T**ampering (англ. Фальсификация).
- **R**epudiation (англ. Отказ от действий).
- **I**nformation disclosure (англ. Раскрытие информации).
- **D**enial of service (англ. Отказ в обслуживании).
- **E**scalation of privileges (англ. Повышение привилегий).

Спуфинг

Угроза спуфинга – угроза, при которой один человек или программа успешно маскируется под другую путём фальсификации данных и позволяет получить незаконные преимущества. Большинство систем безопасности предусматривают обязательную идентификацию и аутентификацию пользователей. Типичные угрозы спуфинга нацелены на слабые механизмы аутентификации, например, при использовании для аутентификации простых коротких паролей или личной информации, которую можно легко найти, например, дату или место рождения.

Фальсификация

Угроза заключается в возможности нарушения целостности информации, приводящая к ее искажению или модификации, путём осуществления нарушителем деструктивного программного воздействия на систему. Реализация данной угрозы возможна в случае получения

[13] Качественный обзор методологий моделирования угроз безопасности ПО – https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

[14] “The Threats to Our Products” – https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

нарушителем системных прав на запись данных. Только авторизованные пользователи должны иметь возможность изменять систему или данные.

Отказ от действий

Злоумышленники часто хотят скрыть свою вредоносную деятельность, чтобы их не обнаружили и не заблокировали. Поэтому они могут пытаться отказываться от своих совершенных действий, например, удалив их из журналов или замаскировавшись под другого пользователя.

Раскрытие информации

Многие системы содержат конфиденциальную информацию, и злоумышленники часто стремятся заполучить ее. Угроза раскрытия информации связана с нарушением конфиденциальности информации. Угроза раскрытия информации относится к утечкам данных. Это может произойти с данными в процессе как в процессе их передачи, так и в состоянии покоя.

Отказ в обслуживании

Угроза отказа в обслуживании направлена на систему с целью довести её до отказа, то есть на создание таких условий, при которых легитимные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам, либо этот доступ будет затруднён. Отказ системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.) или являться способом шантажа и вымогательства денег у владельца системы.

Повышение привилегий

Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему путём эксплуатации неправомерно полученных нарушителем привилегий, подмены пользователя с более высокими привилегиями или путем подмены системы для изменения своих собственных привилегий. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации).

В таблице 6 представлены сведения о том, к нарушению каких свойств системы приводит каждая из угроз.

Таблица 6 – Нарушение свойств системы

Угроза	**Свойство системы**
Спуфинг	Достоверность
Фальсификация	Целостность
Отказ от действий	Неотказуемость
Раскрытие информации	Конфиденциальность
Отказ в обслуживании	Доступность
Повышение привилегий	Авторизация

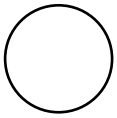
5.1 Методология

Первый шаг в моделировании угроз по модели STRIDE – это смоделировать систему в виде диаграммы потоков данных (англ. Data Flow Diagram – DFD). При моделировании необходимо идентифицировать объекты, события и границы системы. Точность диаграммы потоков данных является ключевым фактором в построении качественной модели угроз.

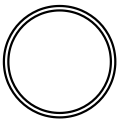
Синтаксис диаграммы потоков данных для построения модели угроз состоит из следующих элементов:

– границы доверия

– внешняя сущность



– процесс



– мульти-процесс

– хранилище данных

– поток данных

– двунаправленный поток данных

– значки активов, мер и угроз

Adam Shostack в книге «Threat modeling. Designing for security»[15] советует придерживаться следующих рекомендаций при построении диаграммы:

[15] Threat modeling. Designing for security – https://threatmodelingbook.com/

– отразите события, которые управляют системой, и покажите процессы, которые ими управляются;

– определите, какие ответы генерируют процессы и как они их отправляют;

– определите источники данных для каждого запроса и ответа;

– определите получателя каждого ответа.

При построении диаграммы, особенно в отношении сложных систем, рекомендуется соблюдать баланс и по возможности разбивать диаграмму на несколько частей или даже стараться упростить ее. Например, если два элемента диаграммы эквивалентны с точки зрения безопасности (находятся внутри одной и той же границы доверия, полагаются на одну и ту же технологию и обрабатывают данные одного типа), то их можно объединить.

Главное, что следует помнить, это то, что диаграмма предназначена для того, чтобы систему можно было понять. Поэтому, когда вы добавляете все новые и новые элементы диаграммы, не спрашивайте: «Правильно ли я делаю?». Вместо этого спросите: «Поможет ли мне это понять, что в системе может пойти не так?».

Пример

На рисунке 1 в качестве примера приведена диаграмма потоков данных простейшей системы платежей.

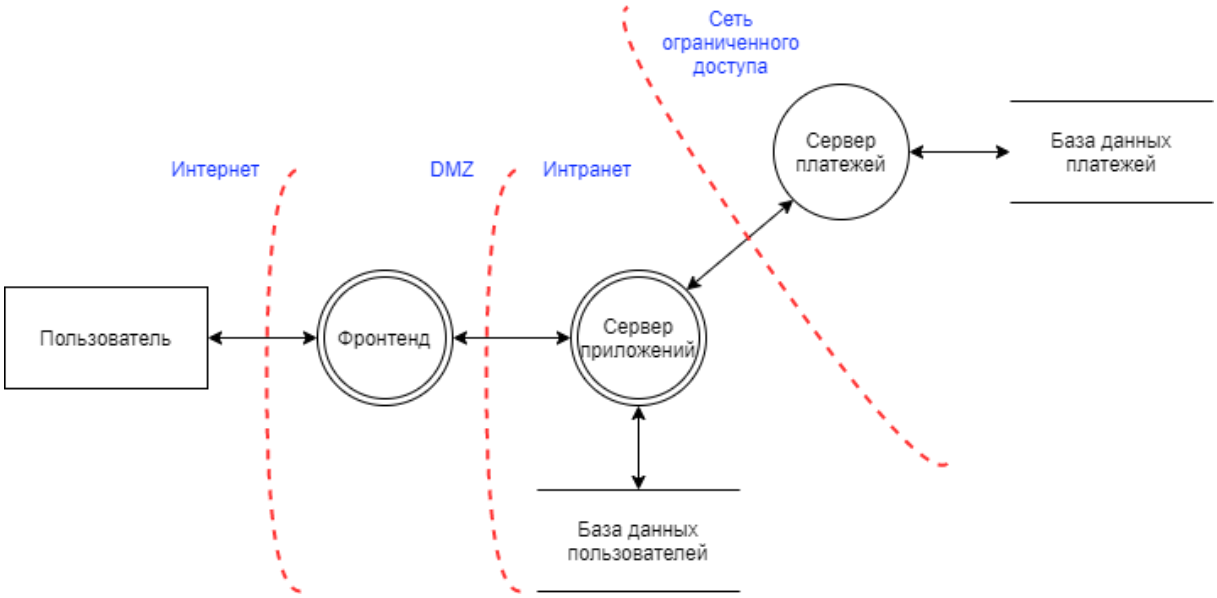


Рисунок 1 – Диаграмма потоков данных простейшей системы платежей

На втором шаге необходимо идентифицировать угрозы по модели STRIDE. Таблицы ниже предоставляют необходимые для этого примеры.

Таблица 7 – Spoofing – Спуфинг | Нарушает: достоверность

Притворяться чем-то или кем-то кроме себя	
Типичные цели DFD	Лучший пример
Процессы, внешние сущности, люди	Ложно утверждать, что ты – Google.com, `lsass.exe`[16], врач-гинеколог[17] или «руководитель головной компании»[18]
Пример угрозы	Что делает атакующий и его методики
Спуфинг процесса на машине	Создает файл первее реального процесса
	Изменяет пути/символьные ссылки
	Переименовывает файлы
Спуфинг файла	Создает файл в директории
	Создает символьные ссылки
	Создает большое количество файлов в предполагаемых директориях работы программы
Спуфинг машины	ARP спуфинг
	IP спуфинг
	DNS спуфинг
	Компрометация DNS
	IP перенаправление
Спуфинг человека	Подделка поля «Email from»
	Завладение реальным аккаунтом

Таблица 8 – Tampering – Фальсификация | Нарушает: целостность

Изменение чего-либо на диске, в памяти или при передаче по сети	
Типичные цели DFD	Лучший пример
Хранилища, потоки данных, процессы	Изменение бинарного файла или содержимого базы данных на диске. Модификация пакетов при передаче по сети. Изменение данных, которые в настоящее время использует программа
Пример угрозы	Что делает атакующий и его методики
Фальсификация файла	Изменяет файл, которым владеет
	Изменяет файл, которым владеете вы
	Изменяет файл на принадлежащем вам файловом сервере
	Изменяет файл на принадлежащем ему файловом сервере
	Изменяет ссылки и перенаправления
Фальсификация памяти	Модифицирует ваш код
	Модифицирует данные, посылаемые вашему API
Фальсификация при передаче по сети	Перенаправляет поток данных на свою машину
	Изменяет передаваемые по сети данные
	Усиливает спуфинговые атаки

[16] Lsass.exe – https://www.securitylab.ru/processinfo/384033.php

[17] Подросток притворялся врачом в отделении гинекологии в клинике США – https://ria.ru/20150116/1042910537.html

[18] Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case – https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Таблица 9 – Repudation – Отказ от действий | Нарушает: неотказуемость

Утверждение пользователя о том, что он не совершал каких-либо действий. Такой отказ и вправду может не быть ложным – ключевой вопрос разработчикам системы: «А какие у вас доказательства?»	
Типичные цели DFD	Лучший пример
Процессы	«Я не нажимал на эту кнопку» или «Я не отправлял этот файл»
Пример угрозы	Что делает атакующий и его методики
Отказ от действия	Заявляет, что он ничего не нажимал
	Заявляет, что он ничего не получал
	Утверждает, что стал жертвой мошенничества
	Использует чужие аккаунты
	Использует чужие платежные инструменты без авторизации
Атака на логи	Замечает, что вы не ведете логи
	Проводит атаку на логи, чтобы переполнить их, вывести из строя или сделать менее читаемыми для проверяющей стороны

Таблица 10 – Information Disclosure – Раскрытие информации

Нарушает: конфиденциальность

Предоставление информации неавторизованному для этого лицу	
Типичные цели DFD	Лучший пример
Процессы, хранилища, потоки данных	Очевидным примером является предоставление доступа к файлам, электронной почте или базам данных (например, атака Forced browsing[19]). Сюда также можно отнести раскрытие информации через сообщения об ошибках или даже раскрытие содержимого памяти программы
Пример угрозы	Что делает атакующий и его методики
Раскрытие информации о процессе	Извлекает чувствительную информацию из сообщений об ошибках
	Извлекает вспомогательную информацию из ошибок, что позволит ему провести более мощные атаки в дальнейшем
Раскрытие информации о хранилищах	Получает доступ из-за отсутствия механизмов ACL[20]
	Получает преимущество из-за неправильных разрешений в базе данных
	Находит файлы, которые были сокрыты[21]
	Находил криптографические ключи на диске (или в памяти)
	Получает ценную информацию из имен файлов
	Читает файлы при их передаче по сети
	Получает данные из логов и временных файлов
	Получает данные из файла подкачки или других временных хранилищ
	Получает данные, завладев устройством и загрузившись с

[19] OWASP Forced browsing – https://owasp.org/www-community/attacks/Forced_browsing
[20] ACL – Access Control List
[21] Security through obscurity – это нехорошо…

	live-образа
Раскрытие информации о потоках данных	Читает данные из сети
	Перенаправляет трафик для чтения данных
	Получает чувствительную информацию анализируя трафик
	Изучает историю взаимодействий, просматривая DNS
	Находит взаимосвязи с помощью раскрытия информации через социальные сети

Таблица 11 – Denial of Service – Отказ в обслуживании

Нарушает:	доступность

Исчерпание ресурсов, необходимых легитимным пользователям	
Типичные цели DFD	Лучший пример
Процессы, хранилища, потоки данных	Программа, которая может прийти в состояние исчерпания всей памяти, файл, который заполняет все дисковое пространство или большое количество сетевых подключений, которое не пропускает реальный сетевой трафик
Пример угрозы	Что делает атакующий и его методики
Отказ в обслуживании процессом	Исчерпывает память и дисковое пространство
	Исчерпывает ресурсы процессора
	Использует процесс как усилитель атаки
Отказ в обслуживании хранилищем	Переполняет хранилище
	Делает большое количество запросов, достаточных для замедления системы
Отказ в обслуживании потоком данных	Исчерпывает сетевые ресурсы

Таблица 12 – Elevation of Privilege – Повышение привилегий

Нарушает:	авторизацию

Позволять сущности делать то, на что у нее нет прав	
Типичные цели DFD	Лучший пример
Процессы	Обычный пользователь выполняет код от имени администратора. Удаленное выполнение кода без авторизации
Пример угрозы	Что делает атакующий и его методики
Повышение привилегий процесса при помощи его порчи	Получает доступ к памяти на чтение/запись некорректно
	Посылает входные данные, которые не могут быть корректно обработаны
Повышение привилегий через некорректные процессы авторизации	
Повышает привилегии через подмену данных	

На третьем этапе необходимо оценить риски от реализации угроз и принять решение по каждому активу – избежать риск, обработать, принять, передать или проигнорировать. При обработке риска необходимо выбрать характерные для каждой угрозы меры противодействия. Это могут быть как стандартные меры, так и меры по изменению проекта архитектуры программного обеспечения или свои собственные меры.

Пример

На рисунке 2 приведена дополненная угрозами и противодействиями диаграмма потоков данных простейшей системы платежей. В таблицах 13, 14 и 15 перечислены идентифицированные активы, угрозы и меры соответственно.

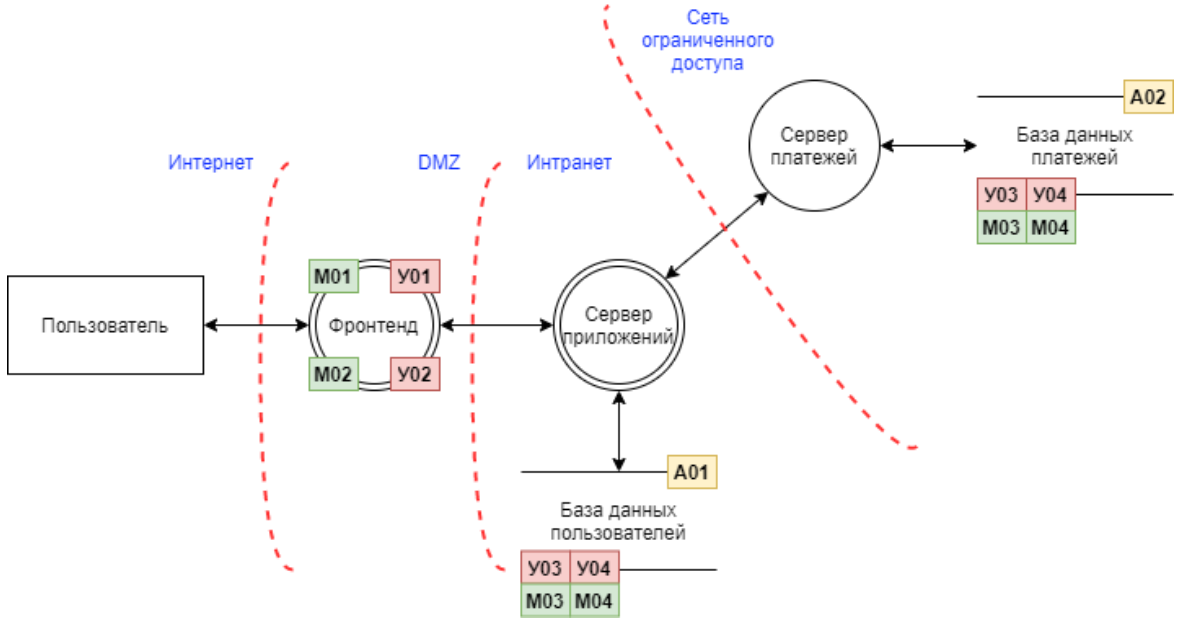


Рисунок 2 – Диаграмма потоков данных простейшей системы платежей

Таблица 13 – **Активы**	
A01	Учетные данные пользователей
A02	Платежные данные

Таблица 14 – **Угрозы**	
У01	Компрометация веб-сайта через XSS
У02	Перехват учетных данных
У03	Повреждение БД
У04	SQL-инъекции

Таблица 15 – **Меры противодействия**	
M01	Санитизация вводимых данных
M02	SSL
M03	Резервирование на удаленный хост
M04	Построение подготовленных выражений (prepared statements)

6 ЛАБОРАТОРНАЯ РАБОТА

Выберите один из предложенных ниже типов программных продуктов. Постройте диаграмму потоков данных для выбранного продукта. Идентифицируйте угрозы, которые могут возникнуть вследствие его применения. Предложите противодействия по каждой угрозе.

Программные продукты:

1. Система управления предприятием.
2. Средство антивирусной защиты с централизованным управлением.
3. Система контейнеризации.
4. Система сбора логов.
5. Система централизованного обновления машин.
6. Система биометрической идентификации.
7. Система сбора и расчета аналитики.
8. Система распределенного контроля версий.
9. Система централизованного контроля версий.
10. Гипервизор (1-го или 2-го типа).

Для построения диаграммы потоков данных рекомендуется использовать библиотеку `threatmodeling` для продукта Draw.io. Для использования выполните следующие шаги:

11. Скачайте и установите Draw.io по ссылке https://about.draw.io/integrations/#integrations_offline
12. Клонируйте репозиторий https://github.com/michenriksen/drawio-threatmodeling
13. В Draw.io создайте новую диаграмму
14. Нажмите «Файл (File)» – «Открыть библиотеку (Open library)». Выберите XML файл из клонированного проекта.

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определение понятию «сертификация».
2. Назовите основные нормативно-правовые акты в области сертификации.
3. Из каких участников состоит система сертификации ФСТЭК России?
4. Сколько оценочных уровней доверия к средствам устанавливает ГОСТ Р ИСО/МЭК 15408-3?
5. Сколько существует уровней доверия по Приказу ФСТЭК №131? Какие из них относят к информации, содержащей сведения, составляющие государственную тайну?
6. Для чего нужны требования доверия?
7. Из каких пунктов состоят требования к проведению испытаний средства?
8. Какие виды тестирования существуют и в чем их отличие? Приведите примеры средств тестирования.
9. Из каких пунктов состоят требования к поддержке безопасности средства?
10. Что описано в ГОСТ Р 56939-2016? Знаете ли вы подобные зарубежные практики?
11. Дайте определение понятию «модель угроз». Что включает в себя процесс моделирования угроз?
12. Какие методологии моделирования угроз вам известны?

ЗАКЛЮЧЕНИЕ

Данное учебно-методическое пособие призвано помочь студентам, изучающим в рамках своей образовательной программы дисциплину «Технология сертификации средств защиты информации», эффективнее освоить изучаемый материал – законодательство в области сертификации средств защиты информации, виды сертификации, участников сертификации, уровни доверия и предъявляемые требования к ним.

Лабораторная работа, включенная в состав данного учебно-методического пособия, призвана помочь понять, как на практике необходимо строить описание программного обеспечения в виде диаграмм потоков данных и определять угрозы безопасности информации, возникающие вследствие применения программного обеспечения по методике STRIDE.

СПИСОК ЛИТЕРАТУРЫ

1. О техническом регулировании [Электронный ресурс] : федеральный закон Российской Федерации от 27 дек. 2002 г. № 184-ФЗ, ред. от 29.07.2017 – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/ (08.11.2019).
2. О сертификации средств защиты информации [Электронный ресурс] : Постановление Правительства РФ от 26 июня 1995 г. № 608, ред. от 21.04.2010 г. – Режим доступа: http://base.garant.ru/102670/ (08.11.2019).
3. О системе сертификации средств защиты информации [Электронный ресурс]: Положение, утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55 – Режим доступа: https://fstec.ru/component/attachments/download/1883 (08.11.2019).
4. Об особенностях оценки соответствия оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения указанной продукции [Электронный ресурс] : Постановление Правительства Российской Федерации от 11.10.2012 № 1036 (с изменениями на 30.04.2019) – Режим доступа: http://docs.cntd.ru/document/902374915 (08.11.2019).
5. ГОСТ Р ИСО/МЭК 15408-3-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности» от 01.09.2014 [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200105711 (08.11.2019).
6. Барабанов А.В., Марков А. С., Цирлов В.Л. Международная сертификация в области информационной безопасности [Текст] / Стандарты и качество. 2016. № 7. С. 30-33.
7. Горюнов М. Н., Юдичев Р. М., Фадин А.А. Внедрение сертификации в жизненный цикл программного обеспечения [Текст] / Защита информации. Инсайд. 2016. № 3 (69). С. 28-35.
8. Марков А. С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации [Текст] / Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
9. Горюнов М. Н., Юдичев Р. М., Фадин А.А. Внедрение сертификации в жизненный цикл программного обеспечения [Текст] / Защита информации. Инсайд. 2016. № 3 (69). С. 28-35.
10. Марков А. С., Шеремет И. А. Теоретические аспекты сертификации средств защиты информации [Текст] / Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.

11. Threat modeling for drivers [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers
12. Shostack A., Threat Modeling: Designing for Security / Wiley. 2014.

Бегаев Алексей Николаевич
Кашин Семен Владимирович
Маркевич Никита Алексеевич
Марченко Алина Андреевна
Павлов Денис Дмитриевич

Сертификация программного обеспечения по требованиям доверия

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49