Международный союз электросвязи

# МСЭ-Т X.1214

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2018)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

# Методы оценки безопасности в сетях электросвязи/информационно-коммуникационных технологий

Рекомендация МСЭ-Т X. 1214

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

**СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ**

| | |
|---|---|
| СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ | X.1–X.199 |
| ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ | X.200–X.299 |
| ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ | X.300–X.399 |
| СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ | X.400–X.499 |
| СПРАВОЧНИК | X.500–X.599 |
| ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ | X.600–X.699 |
| УПРАВЛЕНИЕ В ВОС | X.700–X.799 |
| БЕЗОПАСНОСТЬ | X.800–X.849 |
| ПРИЛОЖЕНИЯ ВОС | X.850–X.899 |
| ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА | X.900–X.999 |
| БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ | |
| Общие аспекты безопасности | X.1000–X.1029 |
| Безопасность сетей | X.1030–X.1049 |
| Управление безопасностью | X.1050–X.1069 |
| Телебиометрия | X.1080–X.1099 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Безопасность многоадресной передачи | X.1100–X.1109 |
| Безопасность домашних сетей | X.1110–X.1119 |
| Безопасность подвижной связи | X.1120–X.1139 |
| Безопасность веб-среды | X.1140–X.1149 |
| Протоколы безопасности | X.1150–X.1159 |
| Безопасность одноранговых сетей | X.1160–X.1169 |
| Безопасность сетевой идентификации | X.1170–X.1179 |
| Безопасность IPTV | X.1180–X.1199 |
| БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА | |
| **Кибербезопасность** | **X.1200–X.1229** |
| Противодействие спаму | X.1230–X.1249 |
| Управление определением идентичности | X.1250–X.1279 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Связь в чрезвычайных ситуациях | X.1300–X.1309 |
| Безопасность повсеместных сенсорных сетей | X.1310–X.1319 |
| Безопасность "умных" электросетей | **X.1330–X.1339** |
| Сертифицированная электронная почта | X.1340–X.1349 |
| Безопасность интернета вещей (IoT) | X.1360–X.1369 |
| Безопасность интеллектуальных транспортных систем (ИТС) | X.1370–X.1389 |
| Безопасность технологии распределенного реестра | X.1400–X.1429 |
| Протоколы безопасности | X.1450–X.1459 |
| ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ | |
| Обзор кибербезопасности | X.1500–X.1519 |
| Обмен информацией об уязвимости/состоянии | X.1520–X.1539 |
| Обмен информацией о событии/инциденте/эвристических правилах | X.1540–X.1549 |
| Обмен информацией о политике | X.1550–X.1559 |
| Эвристические правила и запрос информации | X.1560–X.1569 |
| Идентификация и обнаружение | X.1570–X.1579 |
| Гарантированный обмен | X.1580–X.1589 |
| БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ | |
| Обзор безопасности облачных вычислений | X.1600–X.1601 |
| Проектирование безопасности облачных вычислений | X.1602–X.1639 |
| Передовой опыт и руководящие указания в области облачных вычислений | X.1640–X.1659 |
| Обеспечение безопасности облачных вычислений | X.1660–X.1679 |
| Другие вопросы безопасности облачных вычислений | X.1680–X.1699 |

*Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.*

# Рекомендация МСЭ-Т X.1214

## Методы оценки безопасности в сетях электросвязи/информационно-коммуникационных технологий


**Резюме**

В Рекомендации МСЭ-Т X.1214 приведено описание методики оценки безопасности элементов программного обеспечения сетей электросвязи/информационно-коммуникационных технологий (ИКТ) и примеров передового опыта для использования разработчиками, производителями, операторами и экспертами по безопасности в области электросвязи при решении вопросов безопасности соответствующих элементов программного обеспечения. Как традиционные сети с коммутацией каналов, так и пакетные сети подвержены различным угрозам и атакам, исходящим из внешних и внутренних источников и нацеленным на различные части сети электросвязи/ИКТ. Настоящая Рекомендация охватывает следующее:

– обнаружение уязвимостей в сетях электросвязи/ИКТ;

– методику оценки безопасности в сетях электросвязи/ИКТ.



**Хронологическая справка**

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1214 | 29.03.2018 г. | 17-я | 11.1002/1000/13404 |

**Ключевые слова**

Бинарный анализ, фаззинг, тестирование на возможность проникновения, оценка безопасности, тестирование безопасности, анализ исходных кодов, сканирование уязвимостей


* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

## ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

**Содержание**

**Введение**

Сети электросвязи/ИКТ играют важнейшую роль в экономическом росте большинства стран. Ввиду этого государство осуществляет регулирование отрасли электросвязи, которое включает требования по обеспечению безопасности оборудования и сетей электросвязи. Операторам электросвязи следует принимать надежные и управляемые программы безопасности, для того чтобы обеспечить защиту элементов программного обеспечения своих сетей от внешних и внутренних вредоносных атак, обеспечивая при этом соблюдение местных регуляторных норм. Для этого необходимо иметь весьма эффективный механизм оценки безопасности таких элементов, основанный на принятых на глобальном уровне стандартах и примерах передового опыта в области безопасности.

Поддержание устойчивой системы безопасности в сети организации при постоянно меняющемся характере угроз является сложной и трудоемкой задачей. Восстановление после нарушения безопасности может потребовать от организаций значительных расходов. Эти затраты связаны с деятельностью по ликвидации последствий нарушения, программами защиты и удержания клиентов, юридическими мероприятиями, недовольством деловых партнеров, снижением производительности труда работников и сокращением доходов. Эффективный способ оценки безопасности поможет избежать этих финансовых проблем благодаря упреждающему определению рисков для программных средств и возможностей и принятию соответствующих мер до осуществления атак или нарушения безопасности. Независимая оценка в части безопасности становится все более востребованной среди участников рынка, таких как органы государственного управления, финансовый сектор и сектор электросвязи.

Настоящая Рекомендация посвящена в основном методам оценки безопасности, которые могут применять операторы сетей и поставщики услуг электросвязи/ИКТ для упреждающей идентификации и оценки уязвимостей в соответствующих элементах программного обеспечения.

# Рекомендация МСЭ-Т X.1214

## Методы оценки безопасности в сетях электросвязи/ информационно-коммуникационных технологий

### 1 Сфера применения

В настоящей Рекомендации рассматриваются методы оценки безопасности, которые могут применяться в отношении элементов программного обеспечения сетей электросвязи/информационно-коммуникационных технологий (ИКТ). Как традиционные сети с коммутацией каналов, так и сети следующих поколений с коммутацией пакетов подвержены различным угрозам и атакам, исходящим из внешних и внутренних источников и нацеленным на различные части элементов программного обеспечения сети электросвязи/ИКТ. Оценка безопасности компонентов программного обеспечения до их установки в этих сетях может помочь операторам и поставщикам услуг значительно повысить надежность сетей. Это обусловило потребность в стандартизации в данной области, для того чтобы разработчики, производители, операторы и эксперты по безопасности могли использовать разработанные на глобальном уровне стандарты и примеры передового опыта по оценке безопасности элементов программного обеспечения.

Представленные методы могут использоваться по отдельности или в сочетании, в зависимости от требований или случая.

### 2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2014 год), *Общеизвестные уязвимости и незащищенность*.

[ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 год), *Перечень общеизвестных слабых мест*.

[ITU-T X.1544] Рекомендация МСЭ-Т X.1544 (2013 год), *Перечень и классификация общеизвестных схем атак.*

### 3 Определения

#### 3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

**3.1.1 Репозиторий (repository)** [ITU-T X.1524] – явная или неявная совокупность элементов слабых мест в системе безопасности программного обеспечения, поддерживающая средство, например база данных слабых мест в системе безопасности, набор образцов в анализаторе кода или веб-сайт.

**3.1.2 Уязвимость (vulnerability)** [ITU-T X.1520] – любое слабое место в программном обеспечении, которое может быть использовано для нарушения системы или содержащейся в ней информации.

**3.1.3 Слабое место (weakness)** [ITU-T X.1524]) – дефект или изъян в программном коде, проекте, архитектуре или развертывании программного обеспечения, который может в определенный момент стать уязвимостью или привести к возникновению других уязвимостей.

### 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

**3.2.8 Бинарный анализ (binary analysis)**: Метод выявления слабых мест в исполняемых файлах, написанных на машинном языке.

**3.2.2 Фаззинг (fuzzing)**: Метод обнаружения неизвестных уязвимостей или уязвимостей "нулевого дня" в программном обеспечении путем ввода в него неожиданных данных и мониторинга появления исключений.

**3.2.3 Мутация (mutation)**: Искажение отдельных байтов, слов или строк во входном пакете данных.

**3.2.4 Тестирование на возможность проникновения (penetration testing)**: Метод оценки последствий использования выявленных уязвимостей.

**3.2.5 Оценка безопасности (security assessment)**: Развернутое исследование в целях выявления уязвимостей и рисков в области безопасности.

**3.2.6 Сканирование на основе анализа сигнатур (signature based scanning)**: Метод сканирования, при котором содержание цели сравнивается с базой данных ее известных сигнатур для выявления уязвимостей.

Если конкретная сигнатура совпадает, то сканирующий выявляет уязвимость и предлагает меры по ее устранению.

**3.2.7 Анализ исходных кодов (source code review)**: Метод выявления слабых мест в сегментах программного кода, написанного на языках высокого уровня.

**3.2.8 Инструмент (tool)**: Программное приложение или устройство, которое анализирует хост, сеть, часть программного обеспечения, двоичный код, программное приложение или устройство или же иной артефакт и вырабатывает информацию, которая касается уязвимостей, слабых мест или незащищенности, например сканер уязвимостей, фаззер, инструмент анализа исходных кодов, бинарный анализатор или инструмент тестирования на возможность проникновения.

**3.2.9 Сканирование уязвимостей (vulnerability scanning)**: Метод определения известных или опубликованных уязвимостей в рамках цели.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | | |
|---|---|---|---|
| CAPEC | Common Attack Pattern Enumeration and Classification | | Перечень и классификация общеизвестных схем атак |
| CVE | Common Vulnerabilities and Exposures | | Общие уязвимости и незащищенности |
| CWE | Common Weakness Enumeration | | Перечень общеизвестных слабых мест |
| DUT | Device Under Test | | Испытываемое устройство |
| ICT | Information and Communication Technology | ИКТ | Информационно-коммуникационные технологии |
| OS | Operating System | ОС | Операционная система |
| SQL | Structured Query Language | | Язык структурированных запросов |

## 5 Соглашения по терминологии

Отсутствуют.

## 6 Базовая концепция – тестирование безопасности

Весьма вероятно, что в сетях электросвязи/ИКТ используется разнородный набор оборудования от различных поставщиков. Для проведения оценки в целях выявления и анализа слабых мест и уязвимостей безопасности, содержащихся в реализациях программного, аппаратно-программного и

аппаратного обеспечения, необходима высоконадежная программа сертификации от доверенной третьей стороны. Оценка безопасности продукта связана в основном с обнаружением и проверкой присутствующих в нем уязвимостей. Обнаружение уязвимостей можно разделить на две основные категории (см. пункты 6.1 и 6.2).

### 6.1 Обнаружение известных или опубликованных уязвимостей

Уязвимости программного обеспечения ежедневно находят в широко применимых программных продуктах. Эти уязвимости, например общие уязвимости и незащищенности (CVE), публикуются в Национальной базе данных уязвимостей и в ряде других баз данных. Таким образом эффективное управление опубликованными уязвимостями является важным видом деятельности в работе современных предприятий по обеспечению безопасности. Отслеживать вручную все уязвимости, присутствующие в системах, и соответствующим образом их исправлять – задача чрезвычайной сложности. Существуют автоматические инструменты, которые выполняют сканирование на основе анализа сигнатур для обнаружения этих уязвимостей и идентификации их по [b-CVE].

### 6.2 Обнаружение неизвестных уязвимостей или уязвимостей "нулевого дня"

Этот вид обнаружения уязвимостей предполагает обнаружение еще не опубликованных уязвимостей. Существуют различные подходы к выполнению этой задачи, которые имеют свои достоинства и недостатки. Ни один из подходов не является окончательным, и ни один отдельно взятый метод не может раскрыть все возможные уязвимости данной цели. К инструментам и методам, используемым для обнаружения неизвестных уязвимостей или уязвимостей "нулевого дня", относятся фаззеры, инструменты анализа исходных кодов и инструменты бинарного анализа. Подробная информация об этих инструментах приводится в пунктах 7.2–7.5.

## 7 Методы тестирования безопасности

Как отмечалось выше, существуют разнообразные подходы к обнаружению уязвимостей в элементах программного обеспечения, имеющие свои достоинства и недостатки. Ни один отдельно взятый метод не может раскрыть все возможные уязвимости данной цели. Ввиду этого для эффективного механизма оценки обязательно следует принять несколько подходов, которые рассматриваются в пунктах 7.1–7.5.

### 7.1 Сканирование уязвимостей

Сетевой сканер уязвимостей представляет собой устройство или программное обеспечение, используемое для сканирования архитектуры сети и сообщения о любых уязвимостях, обнаруженных в элементах программного обеспечения этой сети. В ходе сканирования уязвимостей выполняется сопоставление информации из базы данных сигнатур уязвимостей с информацией, полученной при сканировании сети, для получения списка уязвимостей, которые, как предполагается, присутствуют в сети. Иногда в сканер встроен также инструмент тестирования на возможность проникновения для обеспечения способности фактической эксплуатации выявленных уязвимостей в целях полномасштабного подтверждения их наличия. Анализ уязвимостей – это процесс оценки степени серьезности выявленных уязвимостей. Как правило, в эксплуатационной среде организаций имеется множество уязвимостей, и некоторые из них создают бóльший риск безопасности, чем другие. Так некоторые уязвимости программного обеспечения в случае их эксплуатации вызывают катастрофические последствия. Ввиду этого важно определять наиболее значительные проблемы и решать их в первую очередь.

Сканирование уязвимостей для оценки уязвимостей программного обеспечения обычно производится в системах, подключенных к интернету, а также во внутренних сетях, не подключенных к интернету.

Используемые для сканирования уязвимостей инструменты, репозитории и услуги должны быть совместимы с CVE согласно требованиям и функциям, описанным в [ITU-T X.1520].

### 7.2 Фаззинг

Фаззинг определяется как метод обнаружения неизвестных уязвимостей или уязвимостей "нулевого дня" в программном обеспечении путем передачи ему неожиданных данных и мониторинга появления исключений. Обычно это автоматический или полуавтоматический процесс, включающий многократное манипулирование данными и их подачу в целевое программное обеспечение для

обработки. Целевое программное обеспечение может быть стеком протоколов, приложением или файлами, в зависимости от чего фаззер может быть фаззером протоколов, фаззером приложений или фаззером файлов. Тот, кто проводит исследования или тестирование, не обязан знать о внутренней работе цели, и поэтому этот подход иногда называют тестированием методом "черного ящика".

Существуют два основных подхода к фаззингу – фаззинг на основе генерации и фаззинг на основе мутации; они описаны соответственно в пунктах 7.2.1 и 7.2.2.

### 7.2.1 Фаззинг на основе генерации

При этом подходе разработка сценариев тестирования начинается с изучения конкретной спецификации для понимания всех поддерживаемых структур данных и диапазонов допустимых значений для каждой. Затем генерируются входные данные для целей, с тем чтобы тестировать пограничные условия или полностью нарушить спецификацию. Создание сценариев тестирования может требовать значительного объема предварительной работы, но имеет то преимущество, что может повторно использоваться для тестирования нескольких реализаций одного и того же протокола или формата файлов.

### 7.2.2 Фаззинг на основе мутации

Фаззеры на основе мутации применяют мутацию к существующим образцам данных в форме захвата пакетов, относящихся к цели, для создания сценариев тестирования. Каждый отдельный байт, отдельное слово или отдельная строка в этом образце искажаются и направляются к цели. Этот подход требует небольшого объема предварительных исследований и может быть разработан за короткий период времени. Вместе с тем это не вполне эффективный подход, так как для достижения достаточного охвата целевого протокола может потребоваться сбор многочисленных образцов данных.

Фаззеры более всего пригодны для поиска проблем, которые могут вызвать аварийное завершение программы, как, например, переполнение буфера, межсайтовый скриптинг, атаки типа "отказ в обслуживании", ошибки формата и инъекции языка структурированных запросов (SQL). Тестирование фаззингом менее эффективно в отношении угроз безопасности, которые не приводят к аварийному завершению программы, таких как шпионское программное обеспечение, некоторые вирусы, "черви", трояны и клавиатурные шпионы.

Используемые для фаззинга инструменты, репозитории и услуги должны быть совместимыми с перечнем общеизвестных слабых мест (CWE) согласно требованиям и функциям, описанным в [ITU-T X.1524].

## 7.3 Анализ исходных кодов

Анализ исходных кодов представляет собой распространенный подход, используемый разработчиками программного обеспечения для поиска слабых мест или дефектов, который также известен как тестирование по методу "белого ящика". Его можно выполнять вручную или с помощью автоматических средств. Учитывая, что системные программы состоят обычно из миллионов строк кода, чисто ручной анализ, как правило, практически неосуществим. Автоматические инструменты являются чрезвычайно ценным ресурсом, который упрощает задачу, но могут выявить только потенциально уязвимые или подозрительные сегменты кода. Иногда требуется анализ с участием человека, чтобы определить, действительно ли значимы обнаруженные проблемы, потому что этот инструмент дает и ложноположительные результаты. Наиболее серьезное ограничение этого подхода обусловлено нежеланием продавцов или производителей раскрывать исходные коды.

Используемые для анализа исходных кодов инструменты, репозитории и услуги должны быть совместимыми с CWE согласно требованиям и функциям, описанным в [ITU-T X.1524].

## 7.4 Бинарный анализ

Оценка безопасности с использованием инструкций на машинном языке вместо исходного кода обычно называется бинарным анализом. Бинарный анализ создает модель поведения, анализируя управление и поток данных приложения через исполняемый машинный код – как его видит злоумышленник. В отличие от инструментов исходного кода, этот подход точно обнаруживает проблемы в основном приложении и распространяет охват на уязвимости, находящиеся в библиотеках третьих сторон, заранее пакетированных компонентах и коде, введенном компилятором или интерпретациями платформы.

Разработка программного обеспечения – это многоуровневый процесс, в ходе которого возрастающее число типов угроз, таких как поступающие от вредоносного кода и инструментов обхода системы защиты, невозможно обнаружить инструментами анализа исходного кода, потому что в исходном коде они не видны. Эти угрозы можно обнаружить, применяя статический бинарный анализ приложения в его окончательном виде.

Используемые для бинарного анализа инструменты, репозитории и услуги должны быть совместимыми с CWE согласно требованиям и функциям, описанным в [ITU-T X.1524].

### 7.5 Тестирование на возможность проникновения

Тест на возможность проникновения представляет собой упреждающую и санкционированную попытку оценить безопасность инфраструктуры путем безопасной эксплуатации уязвимостей системы, в том числе операционной системы (ОС), дефектов протокола и приложений, неверных конфигураций и даже рискованного поведения конечного пользователя. Основной целью тестирования на возможность проникновения является измерение жизнеспособности систем или компромисса с конечным пользователем, а также оценка соответствующих последствий таких инцидентов для задействованных ресурсов или операций. Тесты обычно проводятся с использованием ручных или автоматических технологий для систематического нарушения хода работы серверов, конечных пунктов, веб-приложений, беспроводных сетей, сетевых устройств, мобильных устройств и других потенциальных точек воздействия. Целью теста на возможность проникновения может быть "белый ящик" (предоставляется базовая и системная информация) или "черный ящик" (предоставляется только минимальная информация или не предоставляется никакой информации).

Проведение теста на возможность проникновения позволяет в упреждающем порядке определить наиболее критичные, менее значимые, а также ложноположительные уязвимости. Это обеспечивает организации возможность более грамотно определять приоритеты в деятельности по устранению уязвимостей и применять необходимые обновления для системы безопасности.

Используемые для тестирования на возможность проникновения инструменты, репозитории и услуги должны быть совместимыми с перечнем и классификацией общеизвестных схем атак (CAPEC) согласно требованиям и функциям, описанным в [ITU-T X.1544].

# Дополнение I

## Блок-схема

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Организация методов оценки безопасности в форме блок-схемы является эффективным способом начать процесс оценки безопасности. Для разработки такой блок-схемы можно рассмотреть модель, в которой оценка начинается с наиболее простой части сети и переходит к развернутым в сети комплексным системам. Сначала обеспечивается безопасность исходного кода элементов программного обеспечения, затем приложений и библиотек в системе, далее систем в сети и, наконец, развернутой сети в целом.

Таким образом всю оценку безопасности можно провести в два основных этапа.

i. Первый этап – этап, выполняемый до развертывания, когда цель можно тщательно проверить, используя все рассмотренные методы оценки безопасности, а результаты этой оценки следует использовать для смягчения обнаруженных уязвимостей.

ii. Второй этап – этап, выполняемый после развертывания, когда цель уже функционирует в сети. На этом этапе проверка цели всеми методами оценки может оказаться невозможной. Ввиду этого аналитики безопасности могут прибегать к периодическому сканированию уязвимостей, для того чтобы обеспечить регулярное устранение выявленных после развертывания продукта уязвимостей путем установки патчей и т. д.

На этапе, предшествующем развертыванию, в качестве первого шага можно проанализировать исходные коды элементов программного обеспечения и исправить обнаруженные дефекты. Затем проводится бинарный анализ приложений и библиотек, используемых этими приложениями. За бинарным анализом следует тестирование фаззингом, а на заключительном этапе выполняются сканирование уязвимостей и тестирование на возможность проникновения всех систем. Итоговые заключения и результаты полной оценки следует передать соответствующим разработчикам, с тем чтобы они могли принять корректирующие меры по смягчению всех обнаруженных уязвимостей.

На этапе после развертывания можно проводить периодическое сканирование уязвимостей всей сети. При обнаружении какой-либо уязвимости ее следует устранить.

На рисунке I.1 приведена блок-схема процесса.

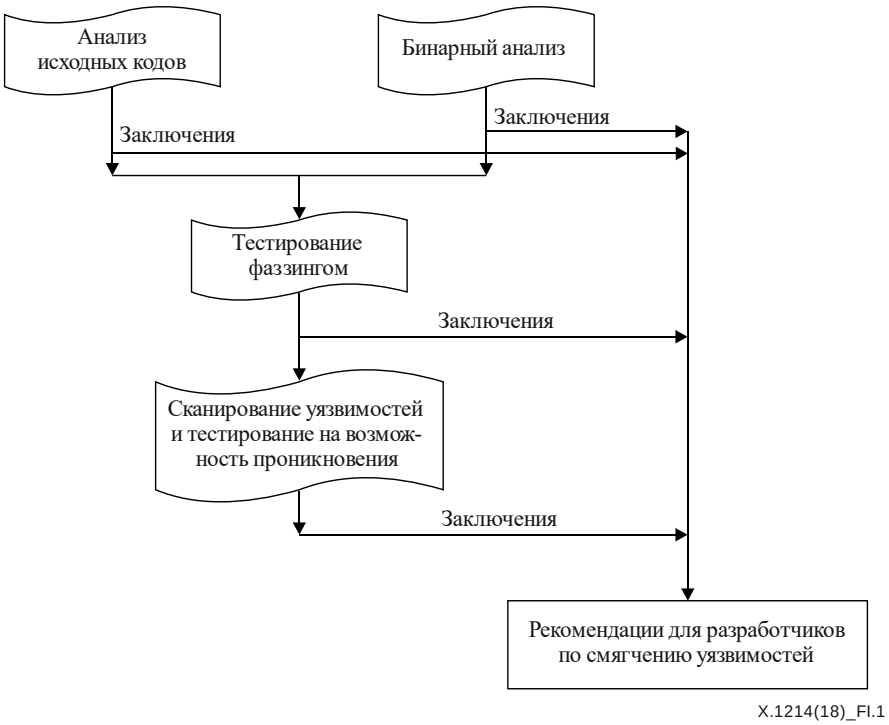


**Рисунок I.1 – Блок-схема методов оценки безопасности**

# Дополнение II

## Другие дополнительные методы повышения безопасности сети ИКТ

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении представлен ряд методов дальнейшего повышения безопасности сети электросвязи/ИКТ.

### II.1 Оценка надежности пароля

В сетях электросвязи/ИКТ широко применяется аутентификация на базе паролей для таких целей, как конфигурирование, управление, эксплуатация и техническое обслуживание, а также предоставление услуг. Надежность этих паролей должны оценивать администраторы системы, с тем чтобы гарантировать сложность их взлома. Для этого можно выполнять раскрытие паролей. Существуют различные механизмы раскрытия паролей, такие как словарные атаки, метод полного перебора и радужные таблицы.

### II.2 Оценка социальной конфиденциальности

В некоторых случаях в отношении работников организаций может применяться психологическое манипулирование, чтобы вынудить их выдать конфиденциальную информацию. Это мошеннический трюк, используемый для сбора информации, обмана или доступа в систему. Для оценки надежности отдельных лиц или групп в организации может применяться социальная инженерия. Конкретные цели могут быть определены, если организация знает о существующей угрозе или полагает, что раскрытие информации каким-либо лицом или конкретной группой лиц может иметь значительные последствия.

### II.3 Оценка функциональной безопасности

Несмотря на то что для тестирования функциональной безопасности не используются какие-либо специальные инструменты, этот подход дополняет методы обнаружения уязвимостей, описанные в пунктах II.1 и II.2.

Для любого устройства или элемента сети, используемого в сетях электросвязи/ИКТ, существуют следующие функциональные требования безопасности:

i) локальная аутентификация пользователя для конфигурирования устройства и управления им;

ii) дистанционная аутентификация пользователя для конфигурирования устройства и управления им;

iii) безопасное хранение пароля в устройстве;

iv) безопасная верификация управления криптографическими ключами;

v) механизм защиты устройства от незаконной установки программных патчей;

vi) дистанционная защита трафика управления устройства;

vii) классификация пользователей управления в соответствии с привилегиями или разрешениями;

viii) безопасная синхронизация времени;

ix) генерация события (журнала) аудита испытываемым устройство (DUT);

x) безопасный экспорт журналов аудита устройством DUT.

### II.4 Беспроводное сканирование

Беспроводное сканирование может помочь организациям принять корректирующие меры для смягчения рисков безопасности, создаваемых беспроводными технологиями. Инструмент беспроводного сканирования должен иметь возможность сканировать все беспроводные устройства стандарта IEEE 802.11 [b-IEEE Std. 8802-11] как на национальном, так и на международном уровнях. С помощью беспроводного сканирования можно обнаруживать несанкционированные беспроводные устройства в диапазоне действия сканеров, определять радиосигналы за пределами периметра организации и выявлять потенциальные обходные пути проникновения в систему и нарушения безопасности.

### II.5 Использование безопасных реализаций криптографических модулей и алгоритмов

Криптографические алгоритмы используются для шифрования и дешифрования данных аутентификации или данных пользователя в целях безопасной передачи данных по сетям электросвязи/ИКТ. Криптографические алгоритмы тщательно разработаны, однако часто встречаются ошибки реализации. Используемые в сетях электросвязи/ИКТ небезопасные алгоритмы, имеющие дефекты реализации, может эксплуатировать злоумышленник, что может привести к значительной потере данных и к действиям по злонамеренному вторжению. Ввиду этого в сетях электросвязи/ИКТ могут использоваться высокозащищенные криптографические модули и алгоритмы.

### II.6 Пассивное прослушивание сети

Прослушивание сети – это пассивный метод, при котором ведется мониторинг связи в сети, декодируются протоколы и анализируются заголовки для выделения представляющей интерес информации. Этот метод также называется монитором сети или анализатором сети и может законным образом использоваться администратором сети или системы для мониторинга сетевого трафика и устранения неисправностей.

С помощью информации, полученной при прослушивании сети, администратор или эксперт по безопасности могут выявлять содержащие ошибки пакеты и использовать данные для определения узких мест и содействия поддержанию безопасной и эффективной передачи данных в сети.

# Библиография


[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – International Standard – Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation. https://cve.mitre.org/cve/

## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|---|---|
| Серия A | Организация работы МСЭ-Т |
| Серия D | Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ |
| Серия E | Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы |
| Серия F | Нетелефонные службы электросвязи |
| Серия G | Системы и среда передачи, цифровые системы и сети |
| Серия H | Аудиовизуальные и мультимедийные системы |
| Серия I | Цифровая сеть с интеграцией служб |
| Серия J | Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов |
| Серия K | Защита от помех |
| Серия L | Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений |
| Серия M | Управление электросвязью, включая СУЭ и техническое обслуживание сетей |
| Серия N | Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ |
| Серия O | Требования к измерительной аппаратуре |
| Серия P | Качество телефонной передачи, телефонные установки, сети местных линий |
| Серия Q | Коммутация и сигнализация |
| Серия R | Телеграфная передача |
| Серия S | Оконечное оборудование для телеграфных служб |
| Серия T | Оконечное оборудование для телематических служб |
| Серия U | Телеграфная коммутация |
| Серия V | Передача данных по телефонной сети |
| **Серия X** | **Сети передачи данных, взаимосвязь открытых систем и безопасность** |
| Серия Y | Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города |
| Серия Z | Языки и общие аспекты программного обеспечения для систем электросвязи |

Отпечатано в Швейцарии
Женева, 2019 г.