**CNSSI № 1253**
27 марта 2014


# КАТЕГОРИРОВАНИЕ И ВЫБОР МЕР БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ЭТА ИНСТРУКЦИЯ ПРЕДПИСЫВАЕТ МИНИМАЛЬНЫЕ СТАНДАРТЫ
ВАШ ДЕПАРТАМЕНТ ИЛИ АГЕНТСТВО МОГУТ ТРЕБОВАТЬ
ДАЛЬНЕЙШЕЙ РЕАЛИЗАЦИИ

# НАЦИОНАЛЬНЫЙ МЕНЕДЖЕР

## ПРЕДИСЛОВИЕ

1. Инструкция № 1253 Комитета по Системам национальной безопасности (CNSS), *Категорирование и выбор мер безопасности для систем национальной безопасности*, предоставляет всем департаментам Федерального правительства, агентствам, бюро и офисам руководство по первым двум шагам Основ управления риском (Risk Management Framework, RMF), Категорирование и Выбор, для систем национальной безопасности (NSS). Эта Инструкция основывается и является сопутствующим документом Специальной публикации (SP) 800-53 Национального института стандартов и технологий (NIST), *Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций*; поэтому она отформатирована так, чтобы соответствовать системе нумерации секций этого документа. Эта Инструкция должна использоваться разработчиками по информационной безопасности систем, санкционирующими должностными лицами, высшими директорами по информационной безопасности и другими для выбора и согласования соответствующей защиты для NSS.

2. Полномочие по выпуску этой Инструкцию проистекают из полномочий на основании Директивы по Национальной безопасности 42, *Национальная политика по безопасности телекоммуникационных и информационных систем национальной безопасности*, которая определяет роли и обязанности по обеспечению безопасности NSS в соответствии с действующим законом, E.O. 12333, с дополнениями, и другими Президентскими директивами. Ничто в этой Инструкции не должно изменять или заменять полномочия Директора Национальной разведки.

3. Эта Инструкция заменяет CNSSI № 1253, датированную 15 марта 2012.

4. Все организации члены CNSS должны планировать свой переход к новым версиям этой Инструкции, включая периодические обновления выделенных ресурсов на меры безопасности. При переходе должны составляться новые оверлеи, которые независимо издаются как приложения к Приложению F этой Инструкции.

5. Приложения CNSSI № 1253 будут пересмотрены и административно обновлены, как требуется, на ежеквартальной основе, чтобы отразить изменения по защитите NSS.

6. Дополнительные копии этой Инструкции, могут быть получены из Секретариата CNSS или вебсайта CNSS: https://www.cnss.gov.

**ДЛЯ НАЦИОНАЛЬНОГО МЕНЕДЖЕРА**

**/s/**
**ДЕБОРА А. ПЛАНКЕТТ**

**Секретариат CNSS (IE32). Агентство национальной безопасности. 9800 Savage Road, STE 6716. Ft Meade, MD 20755-6716**
**Офис: (410) 854-6805 Неклассифицировано ФАКС: (410) 854-6814**
**CNSS@nsa.gov**

# ОГЛАВЛЕНИЕ



# ТАБЛИЦА РИСУНКОВ И ТАБЛИЦ

# ГЛАВА ОДИН
# ВВЕДЕНИЕ

CNSS работал с представителями Гражданского, Военного и Разведывательного сообществ, как часть Рабочей группы Объединенной экспертной группы по инициативе преобразования (JTF), чтобы создать унифицированную основу информационной безопасности. В результате этого сотрудничества NIST издал следующие пять трансформированных документов:

- NIST SP 800-30, *Руководство по проведению оценок риска;*
- NIST SP 800-37, *Руководство по применению основ управления рисками к федеральным информационным системам: подход жизненного цикла безопасности;*
- NIST SP 800-39, *Управление риском информационной безопасности: обзор организации, предназначения и информационных систем*;
- NIST SP 800-53, *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*; и
- 800-53A NIST SP, *Руководство по оценке мер безопасности в федеральных информационных системах и организациях: построение эффективных планов оценки безопасности.*

Намерение этих общих основ состоит в том, чтобы улучшить информационную безопасность, усилить процессы управления рисками и поощрить взаимодействие среди федеральных агентств.

## 1.1 НАЗНАЧЕНИЕ И ОБЛАСТЬ

CNSS сотрудничает с NIST, чтобы гарантировать, что NIST SP 800-53 содержит меры безопасности, которые отвечают требованиям NSS[1], и обеспечить общую основу информационной безопасности для американского Федерального правительства. CNSSI № 1253 является сопутствующим документом публикациям NIST, относящимся к категорированию и выбору (т.е., NIST SP 800-53; NIST SP 800-37; NIST SP 800-60, *Руководство по отображению типов информации и информационных систем к категориям безопасности*; и федеральные стандарты обработки информации [FIPS] 199, *Стандарты по категорированию безопасности Федеральной информации и информационных систем*), и применяются ко всем NSS. Эта Инструкция также предоставляет информацию, относящуюся к NSS, по разработке и применении оверлеев для сообщества национальной безопасности, и значений параметров для мер безопасности NIST SP 800-53, которые применимы ко всем NSS.

Для NSS, где имеются различия между документацией NIST и этой Инструкцией, имеет приоритет эта Инструкция.

[1] NIST SP 800-59, *Руководства по идентификации информационной системы как системы национальной безопасности*, предоставляет руководства, разработанные вместе с Министерством обороны, включая Агентство национальной безопасности, для идентификации информационной системы как системы национальной безопасности. Основание для этих руководств - закон об управлении безопасностью Федеральной информации 2002 (Title III, Public Law 107-347, December 17, 2002), который определяет понятие “система национальной безопасности” и предоставляет общеправительственные требования для информационной безопасности.

## 1.2 РАЗЛИЧИЯ МЕЖДУ CNSSI № 1253 И ПУБЛИКАЦИЯМИ NIST

Существенные различия между этой Инструкцией и публикациями NIST, относящиеся к категорированию и выбору, приведены ниже.

- Эта Инструкция не использует концепцию наивысшего значения (HWM) из FIPS 200, *Минимальные требования безопасности для Федеральной информации и информационных систем,* для категорирования информационных систем (см. Раздел 2.1).
- Определения для умеренного и высокого воздействия уточнены по сравнению с предоставленными в FIPS 199 (см. Раздел 3.1).
- Отношение конфиденциальности, целостности и/или доступности к мерам безопасности явно определено в этой Инструкции (см. Приложение D, Таблица D-2).
- Использование оверлеев мер безопасности уточнено в этой Инструкции для сообщества национальной безопасности (см. Раздел 3.2 и Приложение F).

# ГЛАВА ДВА
# ОСНОВНЫЕ ПРИНЦИПЫ

Эта глава представляет фундаментальные концепции, связанные с выбором мер безопасности и классификацией.

## 2.1 АДАПТАЦИЯ NIST SP 800-53 И FIPS 199

CNSS заимствуют NIST SP 800-53, как задокументировано в этой Инструкции, для сообщества национальной безопасности. CNSS заимствуют FIPS 199, устанавливая категорию безопасности для NSS с тремя дискретными компонентами: одно значение воздействия (низкое, умеренное, или высокое) для каждой из трех целей безопасности (конфиденциальность, целостность и доступность). Сохранение этих трех дискретных компонентов, вместо того, чтобы использовать FIPS 200 HWM, предоставляет степень детализации в распределении мер безопасности по базовым наборам и уменьшает потребность в последующей адаптации. Таблица D-1 в Приложении D представляет это в матрице 3 на 3.

## 2.2 ПРЕДПОЛОЖЕНИЯ, ОТНОСЯЩИЕСЯ К БАЗОВЫМ МЕРЫ БЕЗОПАСНОСТИ

Предположения, связанные с базовыми наборами мер безопасности, предназначены, чтобы представлять большинство федеральных информационных систем и служить основанием, чтобы обосновать распределение мер безопасности по базовым наборам. Хотя для некоторых федеральных информационных систем эти особенности не разделяются, более эффективно для организаций начинать с базового набора и адаптировать его, чтобы удовлетворить потребности этих информационных систем. Системы или среды, которые отличается от упомянутых ниже предположений[2], могут потребовать применения оверлея (см. Раздел 3.2.1), или адаптация выбранных мер безопасности и улучшений (см. Раздел 3.2.2).

Эта Инструкция принимает все предположения из NIST SP 800-53, принимая базовые наборы мер безопасности NIST как основу для базовых наборов NSS, определенных в Таблице D-1 в Приложении D. Предположения NIST SP 800-53:

- Информационные системы расположены в физическом окружении.
- Пользовательские данные/информация в информационных системах организации относительно постоянны.
- Информационные системы многопользовательские (или последовательно или одновременно) при использовании.
- Некоторые пользовательские данные/информация в информационных системах организации не являются общими с другими пользователями, у которых есть санкционированный доступ к тем же самым системам.
- Информационные системы существуют в сетевой среде.
- Информационные системы по своей природе - общего назначения.
- У организаций есть структура, ресурсы и инфраструктура, чтобы реализовать меры безопасности.

Эта Инструкция также учитывает предположения, конкретные к NSS через базовые наборы мер безопасности для NSS. Базовые наборы NSS не предназначены, чтобы учесть эти предположения полностью, а скорее в известной степени, которая представляет минимальную защиту, которая должна быть обеспечена. Дополнительные предположения, относящиеся к NSS:

[2] Примеры систем, которые могут отличаться от предположений, включают системы, не расположенные в физическом окружении, системы в среде с ограниченными ресурсами и автономные системы.

- Угрозы посвященного лица существуют в организациях NSS.
- Постоянно развивающиеся угрозы (APTs) актуальны для NSS и могут уже существовать в организациях NSS.
- Дополнительные методы наиболее успешной практики сверх определенных в базовых наборах NIST необходимы, чтобы защитить NSS.

С другой стороны, есть также некоторые возможные ситуации, которые конкретно не учтены в базовых наборах. Они включают:

- Информационными системами обрабатываются, хранятся или передаются классифицированные данные/информация;
- Отдельные данные/информация требуют специализированной защиты на основе федерального законодательства, директив, нормативных документов или политик; и
- Информационные системы должны общаться с другими системами через различные домены защиты.

## 2.3 ОТНОШЕНИЯ МЕЖДУ БАЗОВЫМИ НАБОРАМИ МЕР И ОВЕРЛЕЯМИ

Базовые наборы NSS, которые состоят из базовых наборов NIST SP 800-53 вместе с дополнительными мерами безопасности NIST SP 800-53, требуемые для NSS, и применимые оверлеи вместе составляют начальный набор мер безопасности. Базовые наборы NSS представляют меры безопасности, необходимые, чтобы учесть воздействие на организации или людей, приводящее к потере конфиденциальности, целостности или доступности, как определено категорией безопасности системы. Оверлеи предназначены, чтобы учесть дополнительные факторы (вне воздействия) или отличия от предположений, используемых при создании базовые наборов мер безопасности (см. Раздел 2.2), использование которых определяется при ответе на вопросы применимости в каждом оверлеи.

Оверлеи – отдельные базовые наборы, что означает, что они могут быть применены к любому базовому набору NSS (например, «Высокий – Умеренный - Умеренный» или «Низкий – Низкий - Низкий»). В результате может быть совмещение мер безопасности базового набора NSS и мер безопасности, определенных в оверлеи (оверлеях).[3] Вместе, комбинация базового набора NSS и применимого оверлея (оверлеев) представляет начальный набор мер безопасности для конкретной адаптации к системе.

Все меры безопасности, независимо от источника (базовый набор или оверлей), могут быть адаптированы, чтобы учесть риск, связанный с конкретной системой. Все меры безопасности, от базового набора или оверлея, реализуются в системе и проверяются во время процесса оценки мер безопасности.

[3] Если использование многих оверлеев приводит к конфликтам между приложением и удалёнными мерами безопасности, смотрите для руководства Раздел 3.2.1.

# ГЛАВА ТРИ
# ПРОЦЕССЫ КАТЕГОРИРОВАНИЯ И ВЫБОРА

В этой главе описываются процессы категорирования и выбора мер безопасности. Кроме тех случаев, когда руководство в этом документе отличается от такового в NIST SP 800-37, сообщество национальной безопасности должно реализовывать Шаги категорирования и выбора RMF, непротиворечивые с NIST SP 800-37.

## 3.1 ШАГ 1 RMF: КАТЕГОРИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Для NSS, Задача категорирования безопасности (Шаг 1 RMF, Задача 1-1) является двухступенчатым процессом:

1. Определение значения воздействия: (i) для типа (типов) [4] информации, которая обрабатывается, хранится, передаётся или защищается[5] информационной системой; и (ii) для информационной системы.
2. Определение оверлеев, которые относятся к информационной системе и среде её эксплуатации, чтобы учесть дополнительные факторы (вне воздействия), которые влияют на выбор мер безопасности.

В сообществе национальной безопасности есть понимание того, что при выполнении конкретных задач должны быть ожидаемы некоторые потери. Поэтому для NSS увеличение в FIPS 199 для умеренных и высоких потенциальных значений воздействия интерпретируют так, как будто бы фраза "… *превышающие ожидаемые по предназначению*" приложена в конце предложения в Разделе 3 FIPS 199.

### 3.1.1 Определение значения воздействия для типов информации и информационной системы

При подготовке к выбору и конкретизации соответствующих мер безопасности для информационных систем организации и соответствующей среды их эксплуатации, организации категорируют свою информации и информационные системы. Чтобы категорировать информацию и информационную систему, выполняются следующие работы:

1. Определение всех типов информации, обрабатываемой, хранимой или передаваемой информационной системой, определение предварительных значений воздействия на безопасность и корректировка предварительных значений воздействия на безопасность для типов информации (см. FIPS 199, NIST SP 800-60, Том I, Раздел 4, и NIST SP 800-60, Том II)[6]. Если тип информации не определен в NIST SP Том II 800-60, задокументируйте тип информации в соответствии с руководством в NIST SP 800-60, Том I.[7]
2. Определение категории безопасности для информационной системы (см. FIPS 199), и внесение любых необходимых корректировок (см. NIST SP 800-60, Том I, Раздел 4.4.2). Категория безопасности системы не должна быть изменена или модифицирована, чтобы отразить управленческие решения по использованию более строгих или менее строгих

[4] Тип информации - конкретная категория информации (например, приватная, медицинская, личная, финансовая, следственная, чувствительная к подрядчику, управления безопасностью), определенная организацией или, в некоторых случаях, общественным правом, правительственным распоряжением, директивой, политикой или нормативным документом.

[5] Интерфейсы мер безопасности защищают информацию, которая обрабатывается, хранится или передаётся во взаимодействующих системах. Эта информация должна быть рассмотрена, когда категорируются интерфейсы мер безопасности.

[6] Для значения воздействия на конфиденциальность, каждая организация должна гарантировать, что это категорирование конкретной информации основывается на потенциально худшем случае воздействия на i) её организацию и ii) любую и все другие американские организации с такой же конкретной информацией.

[7] Если необходимо, дополните NIST SP 800-60 руководством, соответствующим организации.

мер безопасности. Руководство по адаптации в Разделе 3.2.2 должно использоваться, чтобы решить эти проблемы.

3. Документирование категорий безопасности в плане обеспечения безопасности.

### 3.1.2 Определение применимых оверлеев

Оверлеи определяют дополнительные факторы (вне воздействия), которые влияют на начальный выбор мер безопасности. По мере разработки оверлеев CNSS, они публикуются как приложения к Приложению F этой Инструкции. Каждый оверлей включает секцию применимости с серией вопросов, используемых, чтобы определить, применим ли оверлей к информационной системе. Рассмотрите вопросы в каждом оверлее, определенном в Приложении F, чтобы определить, применим ли оверлей. Задокументируйте применимый оверлей (наложения) в плане обеспечения безопасности.

## 3.2 ШАГ 2 RMF: ВЫБОР МЕР БЕЗОПАСНОСТИ

Для NSS выбор мер безопасности (Шаг 2 RMF, Задача 2-2) является двухступенчатым процессом:

1. Выбор начального набора мер безопасности.
2. Адаптация начального набора мер безопасности.

### 3.2.1 Выбор начального набора мер безопасности

Как только категория безопасности информационной системы определена, организации начинают процесс выбора мер безопасности. Чтобы определить начальный набор мер безопасности, необходимо выполнить следующие работы:

1. Выбор базового набора мер обеспечения безопасности, определяемых из Таблицы D-1 в Приложении D, соответствующих категории безопасности системы (т.е., значениям воздействия, определенным для каждой цели безопасности [конфиденциальность, целостность и доступность]).
2. Применение некоторого оверлея (оверлеев), идентифицированного как применимого при категорировании безопасности. Если использование множественных оверлеев приводит к конфликтам между применением или исключением мер безопасности, конфликт решает санкционирующее должностное лицо (или уполномоченный), при взаимодействии с владельцем/управляющим информацией, владельцем информационной системы и ответственным за риски (функция).
3. Задокументируйте начальный набор мер безопасности и обоснование для добавления или удаления мер безопасности из базового набора, сославшись на применимый оверлей (оверлеи) в плане обеспечения безопасности.

### 3.2.2 Адаптация начального набора мер безопасности

Организации начинают процесс адаптации, чтобы изменить и выровнять начальный набор мер безопасности для более точного учёта условий, затрагивающих конкретную систему (т.е., условий, связанных с функциями предназначения/деятельности организации, информационными системами или средой эксплуатации). Организации должны исключать меры безопасности только как функцию установленных, основанных на риске определений. Во время процесса адаптации должна быть проведена оценка степени риска – формальная или неформальная. Результаты оценки степени риска предоставляют информацию о необходимости и достаточности мер безопасности и улучшений во время процесса адаптации. Чтобы адаптировать начальный набор мер безопасности,

необходимо выполнить следующие работы:

1. Адаптация начального набора мер безопасности, используя Таблицу D-2, Приложения E, и Раздел 3.2 NIST SP 800-53.[8]
2. Определение, необходимы ли дополнительные, связанные с доверием, меры безопасности для увеличения уровня доверенности в информационной системе. Если да, то адаптируйте соответственно набор мер безопасности. (См. NIST SP 800-53, Приложение E.),
3. Документирование в плане обеспечения безопасности соответствующих решений, принятых во время процесса адаптации, предоставляя подходящее обоснование для этих решений.
4. Документирование и обоснование в плане обеспечения безопасности любых мер безопасности из начального набора мер безопасности, которые не могут или не осуществимы в системе и которые не могут быть заменены компенсирующими мерами безопасности. По усмотрению санкционирующего должностного лица, эта информация может быть включенная в план действий и вех.

[8] [8]Все руководства в NIST SP 800-53, Раздел 3.2 относятся к NSS за исключением подраздела, называющегося “Рассмотрения, связанные с целями безопасности”. Этот подраздел относятся к базовым наборам мер безопасности NIST и не относится к NSS.

# ПРИЛОЖЕНИЕ А
# ОБОЗНАЧЕНИЯ

ЗАКОНЫ, ПОЛИТИКИ, ДИРЕКТИВЫ, НОРМАТИВНЫЕ ДОКУМЕНТЫ, МЕМОРАНДУМЫ, СТАНДАРТЫ И РУКОВОДСТВА

Приложение А предоставляет ссылки, используемые в № 1253 CNSSI.


1. 44 U.S.C. § 3542, январь 2012.
2. Комитет по системам национальной безопасности, Инструкции 4009, Национальный глоссарий информационного доверия, апрель 2010.
3. Публикация 199 Федеральных стандартов обработки информации, *Стандарты по категорированию безопасности федеральной информации и информационных систем*, февраль 2004.
4. Публикация 200 Федеральных стандартов обработки информации, *Минимальные требования безопасности для федеральной информации и информационных систем*, март 2006.
5. Закон об управлении безопасностью федеральной информации (P.L. 107-347, Title III), декабрь 2002.
6. Национальный институт стандартов и технологий, Специальная публикация 800-30, *Руководство по проведению оценок степени риска*, сентябрь 2012.
7. Национальный институт стандартов и технологий, Специальная публикация 800-37, пересмотр 1, *Руководство по применению основ управления рисками к федеральным информационным системам: подход жизненного цикла безопасности*, февраль 2010.
8. Национальный институт стандартов и технологий, Специальная публикация 800-39, *Управление риском информационной безопасности: Обзор организации, предназначения и информационных систем*, март 2011.
9. Национальный институт стандартов и технологий, Специальная публикация 800-53, пересмотр 4, *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*, апрель 2013.[9]
10. Национальный институт стандартов и технологий, Специальная публикация 800-53A, *Руководство по оценке мер безопасности в федеральных информационных системах и организациях: Построение эффективных планов оценки безопасности*, июнь 2010.
11. Национальный институт стандартов и технологий, Специальная публикация 800-59, *Руководство по идентификации информационных систем как систем национальной безопасности*, август 2003.
12. Национальный институт стандартов и технологий специальная публикация 800-60, пересмотр 1, Том I: *Руководство по отображению типов информации и информационных систем к категориям безопасности*, август 2008.
13. Национальный институт стандартов и технологий специальная публикация 800-60, пересмотр 1, Том II: *Приложения к Руководству по отображению типов информации и информационных систем к категориям безопасности*, август 2008
14. Директива 42 по национальной безопасности, *Национальная политика по безопасности телекоммуникационных и информационных систем национальной безопасности*, июль 1990.


[9] Включает исправления добавленные с 7 мая 2013.

# ПРИЛОЖЕНИЕ В
# ГЛОССАРИЙ

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины в этом документе определены в документах NIST JTF и CNSSI № 4009, за исключением упомянутых ниже.

| | |
|---|---|
| Начальный набор мер безопасности | Набор мер безопасности, являющийся результатом комбинации базового набора мер безопасности и применимых оверлеев для адаптации к конкретной системе. |
| Базовые наборы мер безопасности NSS | Комбинация базовых наборов мер безопасности NIST 800-53 (обозначенных «X»), и дополнительных меры безопасности NIST SP 800-53, требуемых для NSS (обозначенных «+»), которые применяются в NSS. |
| Предварительные значения воздействий на безопасность [NIST SP 800-60, Уточнённая] | Начальные или условные определения воздействия, сделанные до всех рассмотрений, полностью пересматриваемые, анализируемые и принимаемые на последующих шагах категорирования соответствующими чиновниками. |
| Расширение мер безопасности | Описание, используемое в оверлеях мер безопасности, которое расширяет основные возможности мер безопасности, определяя дополнительную функциональность, изменяя механизм стойкости или добавляя, или ограничивая параметры реализации. |

# ПРИЛОЖЕНИЕ С
# АКРОНИМЫ

ОБЩИЕ СОКРАЩЕНИЯ

Акронимы и сокращения, используемые в этой Инструкции, включены ниже. Меры, относящиеся к акронимам, включенные в таблицы приложений D и E, определены в NIST SP 800-53.

| | |
|---|---|
| APT | Постоянно развивающаяся угроза |
| CNSS | Комитет по системам национальной безопасности |
| CNSSI | Инструкции Комитета по системам национальной безопасности |
| EO | Правительственное распоряжение |
| FIPS | Федеральные стандарты обработки информации |
| FISMA | Закон об управлении безопасностью федеральной информации |
| HWM | Верхний уровень |
| JTF | Межведомственная рабочая группа объединенной экспертной группы по инициативе преобразования |
| NIST | Национальный институт стандартов и технологий |
| NSS | Система национальной безопасности |
| RMF | Основы управления рисками |
| P.L. | Общественный закон |
| SC | Категория безопасности |
| SDLC | Жизненный цикл разработки систем |
| SP | Специальная публикация |
| США | Соединенные Штаты Америки |
| U.S.C. | Кодекс Соединенных Штатов |

# ПРИЛОЖЕНИЕ D
# ТАБЛИЦЫ МЕР БЕЗОПАСНОСТИ

## D.1 БАЗОВЫЕ МЕРЫ БЕЗОПАСНОСТИ NSS

Таблица D-1 использует матрицу 3x3, чтобы определить применимость мер безопасности NIST SP 800-53, Пересмотр 4 в качестве базовых наборов мер безопасности для NSS. Матрица также определяет, какие дополнительные меры безопасности необходимы для защиты NSS. Эта таблица представляет меры безопасности, применимые к NSS, на основе значений воздействия.

Матрица 3x3 имеет девять колонок, показывая три возможных значения воздействия (низкое, умеренное или высокое) для каждой из трех целей безопасности (конфиденциальность, целостность или доступность). «X»-ы в таблице отражают спецификацию значения воздействия NIST (т.е., низкое, умеренное и высокое). «+»-ы в таблице отражают дополнительные спецификации CNSS значений воздействий для всех NSS. Соответствие мер безопасности целям безопасности детализировано в таблице D-2. Пробел в таблице показывает, что мера безопасности или не выбрана, или не назначена конкретной цели безопасности для назначения этой Инструкции. Обозначение мер обеспечения безопасности - «исключено», означает, что они больше не находятся в каталоге мер безопасности NIST SP 800-53[10].

**Таблица D-1: базовые** меры **безопасности NSS**

Таблица D-1 представлена на страницах D-1…D-35 CNSSI No. 1253.

[10] Изменение каталога мер безопасности, относится к полномочиям NIST.

## D.2 ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ МЕР БЕЗОПАСНОСТИ

Таблица D-2 включает дополнительную информацию о мерах безопасности NIST SP 800-53, включая обоснования по включению в базовые наборы NSS, связанные с конфиденциальностью, целостностью и доступностью, и потенциально общие/наследуемые меры обеспечения безопасности.

Связь конфиденциальности, целостности и доступности с мерами безопасности NIST: цели безопасности конфиденциальность, целостность и доступность определены в 44 United States Code (U.S.C.), Section 3542. Базовые наборы NIST SP 800-53 не характеризует наличие отношений мер безопасности с целями безопасности. Таблица D-2 связывает меры безопасности из NIST SP 800-53, Пересмотр 4, Приложение F с тремя целями безопасности. Эти связи - фактор в разработке Таблицы D-1 и могут использоваться, чтобы предоставить информацию для решений по адаптации.

Основной подход и предположения для связей мер безопасности:

- Каждая мера безопасности и/или улучшение выделяется на основе того, является ли цель (цели) безопасности *основным* назначением меры и/или улучшения. Если цель безопасности только косвенно затрагивается мерой безопасности и/или улучшением, она не связана с этой мерой и/или улучшением.
- Первая мера безопасности в каждом семействе закрывает политику и процедуры для всего семейства, и в большинстве случаев они назначаются всем целям безопасности (конфиденциальность, целостность и доступность).
- Цели конфиденциальность и целостность в основном сосредоточены на чтении и написании (раскрытие и модификация).
- Криптографические методы предоставляют возможность учесть раскрытие (шифруя информацию) и целостность (с помощью хешей и зашифрованных хешей). Поэтому меры безопасности, которые учитывают использование криптографических методов, как правило, назначаются конфиденциальности и целостности.
- Цель целостность также относится к корректности действий.
- Цель доступность, прежде всего, касается жизнеспособности и гарантирует, что ресурсы там, где необходимы.
- Цель доступность также относится к управлению последствиями и противостоянию некоторым действиям, направленным на отказ в обслуживании.

Обоснование для базовых наборов NSS: Меры безопасности, выбранные чтобы учесть предположения для NSS, каждая связана с конкретным обоснованием. Ниже приведены резюме всех обоснований, содержавшихся в Таблице D-2.

- **Угроза посвященного лица**: Эта мера безопасности помогает противостоять/ смягчать угрозы посвященного лица, которые существуют в организациях NSS.
- **APT**: Эта мера безопасности помогает противостоять/смягчать APTs, которые предназначаются для NSS и могут уже существовать в организациях NSS.
- **Лучшая практика NSS**: Эта мера безопасности поддерживает дополнительные методы наиболее успешной практики сверх учтенных в базовых наборах мер NIST и необходима, чтобы защитить системы национальной безопасности.
- **Выпуск: [Выпуск]**: Эта мера безопасности поддерживает текущие и предварительные выпуски CNSS, которые имеют заявления технической политики.

- **В поддержку и/или непротиворечивая с [Мера(ы) безопасности]**: Эта мера поддерживает и/или непротиворечива с другими мерами безопасности и улучшениями мер безопасности в базовых наборах NSS.
- **Предположение NIST [Предположение]**: Эта мера безопасности дополнительно учитывает предположение NIST.
- **В поддержку EO [число]**: Эта мера безопасности поддерживает правительственное распоряжение.
- **Облегчение непрерывного мониторинга**: Эта мера безопасности поддерживает Высшее должностное лицо по обмену информацией и Руководящий комитет по защите в области непрерывного мониторинга.
- **Лучшая практика**: Эта мера безопасности поддерживает промышленные или общие лучшие методы безопасности (эти меры безопасности будут рекомендоваться NIST для включения в базовые наборы).

Потенциально общие/наследуемые меры безопасности: способ, в котором некоторые меры безопасности явно формулируются в описаниях мер безопасности или дополнительном руководстве, подразумевает возможность для реализации как общих мер безопасности. Таблица D-2 определяет меры безопасности, которые могут быть потенциально реализовали как общие меры безопасности. Заключительное определение того, какие меры безопасности будут реализованы как общие меры безопасности варьируется в зависимости от организации, процесса предназначения/деятельности или информационной системы и её намеченной среды/развертывания. Общие меры безопасности, определенные в Таблице D-2, основаны на следующих предположениях:

- Общие меры безопасности, могут быть определены на уровне организации, процесса предназначения/деятельности или информационной системы.
- У организаций есть персонал, определённый для разработки политики и процедур для всей организации.
- Организации имеют установленные сервисы (например, корпоративные, локальные), реализующие технические меры безопасности, которые могут унаследовать другие информационные системы.
- Информационные системы расположены в физических средах, которые предоставляют услуги физической безопасности (например, оружие, ворота и охрану, контроль климата, пожаротушение).
- Границы санкционирования установлены для интерфейсов мер безопасности, которые не включают связанные информационные системы.
- Отдельная граница санкционирования установлена для облачного предприятия.
- Границы санкционирования установлены для некоторых больших сервисов информационных технологий, таких как домены Microsoft Windows, которые включают все информационные системы, которыми управляют в домене. Хотя некоторые компоненты информационных технологий в домене Microsoft Windows могут полагаться на другие компоненты информационных технологий в домене Microsoft Windows, чтобы удовлетворить некоторые меры безопасности способом, подобном наследованию, это различие будет учтено в матрицах отслеживания мер безопасности (SCTMs), вместо того, чтобы описывать, как общие предоставленные и унаследованные меры безопасности.

**Таблица D-2: Дополнительная информация по мерам безопасности**

Таблица D-2 представлена на страницах D-37…D-62 CNSSI No. 1253.

# ПРИЛОЖЕНИЕ E
# ЗНАЧЕНИЯ ПАРАМЕТРОВ МЕР БЕЗОПАСНОСТИ

Таблица E-1 содержит значения параметров, определенные для NSS. Эти значения параметров - минимальные стандарты для NSS. Любые отклонения от этих значений должны быть задокументированы в плане обеспечения безопасности. Если мера безопасности или улучшение меры безопасности не указаны в Таблице E-1:

- У них нет параметра, определяемого организацией;
- Все параметры в рамках меры безопасности не применимы, чтобы определить для всех NSS на уровне CNSS; или
- Они были исключены в NIST SP 800-53.

**Таблица E-1: Значения параметров мер безопасности для NSS**

Таблица E-1 представлена на страницах E-1…E-20 CNSSI No. 1253.

# ПРИЛОЖЕНИЕ F
# ОВЕРЛЕИ

РУКОВОДСТВО ДЛЯ ОСОБЫХ УСЛОВИЙ И ИСПОЛЬЗОВАНИЯ ВСЕМ СООБЩЕСТВОМ

Оверлеи - спецификация мер безопасности, улучшений мер безопасности, дополнительных руководств и другая информация поддержки намерений дополнить (и затем улучшить) базовые меры безопасности, с завершением в начальном наборе мер безопасности. CNSS использует оверлеи, чтобы прийти к согласию в сообществе интересов и определить соответствующие меры безопасности, у которых есть всеобъемлющая поддержка для очень конкретных обстоятельств, ситуаций и/или условий, которые отличаются от предположений в Разделе 2.1. Каждое оверлей представляет руководство по определению, когда он применимо. Оверлей предоставляет спецификации мер безопасности, которые непосредственно применимы к ее предмету.[11]

*Руководство и публикация оверлеев*

CNSS рассматривает и издает все оверлеи, которые будут приложениями к Приложению F CNSSI № 1253. CNSS может также быть включен в разработку таких оверлеев.

Рабочая группа Управления рисками безопасности информационных систем CNSS (ИССРМ WG) управляет процессами инициирования, разработки, санкционирования, публикации и поддержки оверлеев. Когда новые оверлеи изданы, или существующие оверлеи пересмотрены, это приложение административно обновляется. CNSS предоставляет загружаемые копии одобренных и изданных оверлеев,[12] а также шаблон, который будет использоваться в разработке оверлеев (см. Приложение 1), и руководство по разработке оверлеев. Оверлеи, помеченные “Неклассифицировано// Только для служебного пользования” (UNCLASSIFIED//FOUO), доступны на ограниченном вебсайте CNSS.

*Приложения к приложению F (раньше приложение K): Оверлеи, изданные CNSS*

Приложение 1: Шаблон оверлея (1 августа 13)

Приложение 2: Оверлей космической платформы (6 июня 13)

Приложение 3: Оверлей междоменного решения (27 сентября 13)

Приложение 4: Оверлей Разведки (23 октября 12) (Документ - U//FOUO),

Приложение 5: ЗАРЕЗЕРВИРОВАНО

[11] Оверлеи – независимый базовый набор мер; поэтому, они не рассматривают, отобрана ли мера безопасности для какого-либо конкретного базового набора мер. При применении оверлея вместе с выбранным базовым набором мер, может быть много «двойных» мер безопасности. Эти меры безопасности не должны быть реализованы дважды; однако, оверлей предоставляет дополнительные спецификации, соответствующие его теме, и обоснование по процессу адаптации.

[12] Оверлеи изданы на вебсайте CNSS с Инструкциями CNSS, в: https://www.cnss.gov.