ВЕСТНИК
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МОРСКОГО И РЕЧНОГО ФЛОТА ИМЕНИ АДМИРАЛА С. О. МАКАРОВА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.53

С. А. Рудакова,
аспирант,
СПИИРАН

КОНЦЕПЦИЯ ВЫБОРА МЕТРИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE INFORMATION SECURITY METRICS CHOICE CONCEPTION

Предлагается концепция выбора метрик для проведения аудита информационной безопасности, основанная на пошаговом разделении свойства «информационная безопасность». Концепция может быть применена на различных объектах информатизации водного транспорта.

The metrics choice conception for information security audit carrying out based on step-by-step separation of property "information security" is proposed. The conception can be applied in the different aqueous transport information objects.

Ключевые слова: информационная безопасность, аудит, оценка защищенности, метрики информационной безопасности.

Key words: information security, audit, safety assessment, information security metrics.

ИНФОРМАЦИОННУЮ безопасность нельзя рассматривать как готовый продукт, информационная безопасность — это состояние, обеспечиваемое непрерывным процессом защиты информации. Этот процесс может включать различные меры и средства, обеспечивающие информационную безопасность более или менее успешно, выбор мер и средств защиты информации критично важен для достижения информационной безопасности. Основой для такого выбора служат текущее состояние информационной безопасности, сформированное с помощью оцененных метрик информационной безопасности, и цели защиты информации, желаемые для достижения. Статья посвящена метрикам информационной безопасности.

Как правило, для оценки уровня информационной безопасности объекта информатизации используются уже готовые наборы метрик, заданные различными стандартами или составленные экспертами. Неполнота или избыточность такого набора непосредственно влияет на корректность оценки защищенности информации, а значит, и на стратегию развития информационной безопасности, и на выбор мер и средств обеспечения информационной безопасности, и в конечном счете на уровень информационной безопасности объекта информатизации. В связи с этим выбор метрик информационной безопасности — это один из наиболее значимых шагов процесса защиты информации.

Ниже приведены примеры стандартов, действующих на территории РФ в качестве обязательных или предоставляющих готовые наборы метрик информационной безопасности:

— требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом ФСТЭК России от 11.02.13 № 17) [3];

— состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом ФСТЭК России от 18.02.13 № 21) [4];

— обеспечение информационной безопасности организации банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-20xx. Стандарт Банка России СТО БР ИББС-1.2-2010 [6];

— PSI DSS (Payment Card Industry Data Security Standard) [7];

— информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. ГОСТ Р ИСО/МЭК 27001-2006 [1].

Далее приведены примеры стандартов, предлагающих осуществлять выбор метрик информационной безопасности самостоятельно (набор метрик определяет эксперт, аудитор):

— базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. зам. директора ФСТЭК России 15.02.08) [5];

— информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. ГОСТ Р ИСО/МЭК 27004-2011 [2].

Также выбор метрик информационной безопасности осуществляется самостоятельно при оценке эффективности защиты информации или состояния информационной безопасности, не основанной на каких-либо общепринятых стандартах.

В связи с актуальностью вопроса выбора метрик информационной безопасности была разработана соответствующая концепция, описанная ниже.

Целью концепции является определение метрик для проведения аудита информационной безопасности, удовлетворяющих требованиям:

— набор метрик должен быть полным;

— набор метрик должен не иметь избыточностей.

Для достижения этих целей предлагается свойство «безопасность информации» (свойство верхнего уровня), которое необходимо оценить в ходе аудита, разделить на несколько более детализированных свойств (свойства нижнего уровня), соблюдая при этом ряд правил, представленных ниже (правила детализации свойств).

Каждое свойство нижнего уровня предлагается подвергать детализации по правилам детализации свойств (при этом детализируемое свойство становится свойством верхнего уровня) до тех пор, пока оно не будет отвечать требованиям, предъявляемым к метрикам информационной безопасности (представлены ниже).

Пример применения предложенной концепции приведен в конце статьи.

1. Правила детализации свойств

1.1. Правило необходимости свойств.

Должно соблюдаться условие: $L_i \subsetneq H$ при $i = 1, 2, ..., n$,

где L_i — множество характеристик свойства нижнего уровня;

H — множество характеристик свойства верхнего уровня;

n — количество свойств нижнего уровня.

1.2. Правило достаточности свойств.

Должно соблюдаться условие: $\forall A \cap H = \varnothing$ при $A \cap L_i = \varnothing$; $i = 1, 2, ..., n$,

где A — произвольное множество;

H — множество характеристик свойства верхнего уровня;

L_i — множество характеристик свойства нижнего уровня;

n — количество свойств нижнего уровня.

1.3. Правило уникальности свойств.

Должны соблюдаться условия:

1. $L_i \cap L_j = \varnothing$ при $i = 1, 2, ..., n$; $j = 1, 2, ..., n$; $i \neq j$.

2. $L_i \neq \varnothing$ при $i = 1, 2, ..., n$,

где L_i, L_j — множества характеристик свойства нижнего уровня;

n — количество свойств нижнего уровня.

1.4. Правило количества свойств.

Количество свойств нижнего уровня должно быть минимальным, но не менее двух (предлагается использовать 2–5 свойств).

2. Требования к метрикам информационной безопасности

Для того чтобы свойство информации можно было отнести к метрикам информационной безопасности, оно должно отвечать требованиям, представленным в табл. 1.

Таблица 1

Требования к метрикам информационной безопасности

№ п/п	Требование	Пояснение
1	Конкретность	Метрика должна иметь непосредственное отношение к информационной безопасности
2	Измеримость	Должна существовать возможность однозначно количественно измерить метрику (например, по стоимости, или с помощью булевой алгебры)
3	Значимость	Изменение значения метрики должно означать изменение состояния информационной безопасности объекта информатизации

3. Пример применения концепции

На рис. 1 приведен пример применения описанной выше концепции для объекта информатизации.

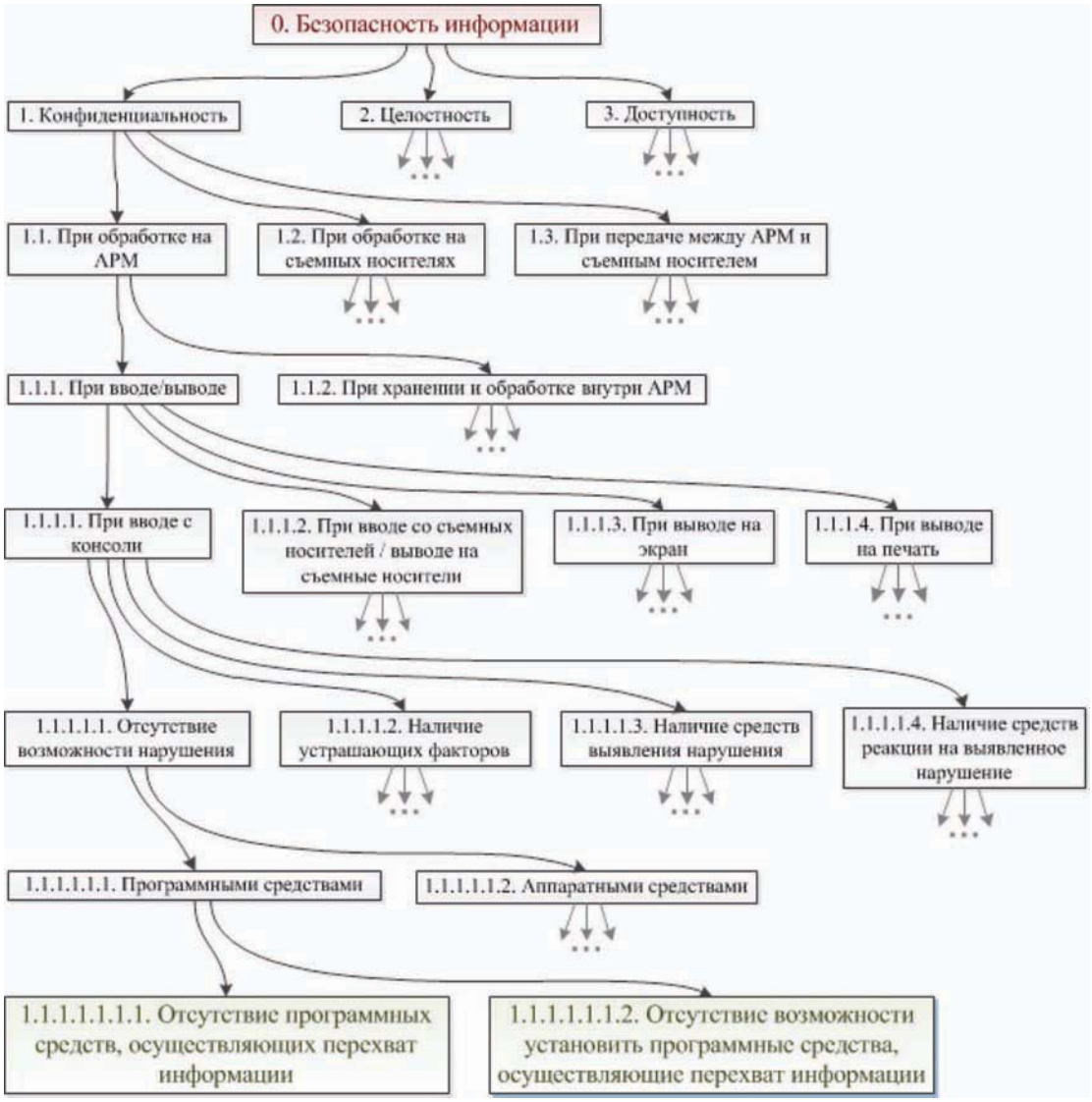

Рис. 1. Пример выбора метрик

Данный объект состоит из:

— двух автономных автоматизированных рабочих мест (АРМ) в защищенном исполнении, каждый из которых включает в свой состав принтер и съемные носители информации (USB-флеш-носители, оптические диски, бумага);

— информации, имеющей различные грифы секретности: «Несекретно», «Секретно», «Совершенно секретно»;

— выделенного помещения;

— персонала, осуществляющего обслуживание объекта информатизации.

При построении этого примера были приняты следующие общепринятые ограничения [8; 9]:

— безопасность информации обеспечивается ее конфиденциальностью, целостностью и доступностью;

— безопасность информации достигается отсутствием возможности нарушения, наличием устрашающих факторов, наличием средств выявления инцидентов и реагирования на выявленные инциденты.

Выводы

Предложенная концепция позволяет определить набор метрик информационной безопасности, который:

— лишен избыточностей за счет правила необходимости свойств;

— является полным (то есть отсутствуют неучтенные метрики) за счет правила достаточности свойств.

Предложенная концепция может найти применение на различных объектах информатизации водного транспорта:

— объектах информатизации, расположенных на суше и непосредственно на водном транспорте;

— типовых и специфических объектах информатизации, используемых для обслуживания водного транспорта;

— объектах информатизации, являющихся частью гражданского и военного, пассажирского и грузового водного транспорта.

Целями применения концепции на водном транспорте могут быть:

— обеспечение защиты открытой информации (например, на объектах информатизации, расположенных на суше и занимающихся гражданскими пассажирскими перевозками);

— обеспечение защиты государственной тайны (например, на военном водном транспорте);

— обеспечение защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (например, защита коммерческой тайны при гражданских грузоперевозках).

Список литературы

1. ГОСТ Р ИСО/МЭК 27001-2006. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

2. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. № 17.

4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18 февраля 2013 г. № 21.

5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. зам. директора ФСТЭК России 15 февраля 2008 г.

6. СТО БР ИББС-1.2-2010.

7. www.pcidss.ru

8. ism3.wordpress.com

9. *Shon H.* CISSP All-in-one Exam Guide / H. Shon. — 2010.