Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056.5

На правах рукописи

БОГАТКО
Максим Павлович

ОЦЕНКА БЕЗОПАСНОСТИ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра технических наук

по специальности 1-38 80 04 Технология приборостроения

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**АЛЕКСЕЕВ Виктор Федорович,** кандидат технических наук, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Рецензент:	**ПОЛУБОК Владислав Анатольевич,** кандидат технических наук, доцент, ведущий инженер-программист Республиканского унитарного предприятия «Центр информационных технологий Национального статистического комитета Республики Беларусь»

Защита диссертации состоится «27» января 2017 г. года в $9^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, 1 уч. корп., ауд. 415, тел.: 293-20-87, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Построение системы информационной безопасности, также, как и информационной безопасности организации требует к себе системного подхода, который предполагает оптимальную пропорцию между организационными, программными, правовыми и физическими свойствами информационной безопасности. В связи с этим в рамках комплексного подхода обеспечения информационной безопасности необходимо использовать качественные (с высоким уровнем обеспечения безопасности информации при обработке, передаче и т.п.) средства защиты информации. Использование таких средств требует проведения оценки их безопасности.

На настоящий момент существует достаточно большое количество работ зарубежных исследователей, рассматривающих оценку безопасности аппаратно-программных средств защиты информации (Камаев В.А., Натров В.В., Коробейников А.Г., Трояков И.Б., Жаринов И.О., Парамонов П. П. и др.).

В исследованиях, представленных в научно-технической литературе, а также в технических нормативно-правовых актах приведены результаты, подтверждающие необходимость проведения оценки безопасности аппаратно-программных средств защиты информации. Среди существующих методов оценки безопасности аппаратно-программных средств в основном выделяют два способа:

1. Определение соответствия техническому заданию на создание средства защиты реализованных функций и задач защиты, эксплуатационных характеристик и требований;

2. Анализ функциональной надежности средств защиты.

В этой связи исследования по теме диссертации, направленные на выбор базисного метода оценки безопасности аппаратно-программных средств защиты информации, являются актуальными.

Выражаю благодарность за оказанную помощь в ходе подготовки диссертационной работы своему научному руководителю, кандидату технических наук, доценту кафедры ПИКС, Алексееву Виктору Федоровичу.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Большинство исследований по теме диссертации направлены на получение информации, подтверждающей необходимость использования аппаратно-программных средств защиты информации, обладающих высоким уровнем обеспечения информационной безопасности. В связи с этим, оценка безопасности аппаратно-программных средств защиты информации является актуальной.

Степень разработанности проблемы

В современных исследованиях, представленных в научно-технической литературе и технических нормативно-правовых актах, приведены методики, модели и этапы проведения оценки безопасности средств защиты информации. Несмотря на это среди существующих методик и моделей отсутствует либо недостаточно полно проработан вопрос оценки аппаратно-программных средств защиты информации. Это обусловлено тем, что существующие типовые методики носят описательный характер, что затрудняет автоматизацию и оптимизацию процессов оценки соответствия средств защиты информации.

Цель и задачи исследования

Цель диссертации состоит в проведении анализа используемых методик и моделей при проведении оценки безопасности аппаратно-программных средств защиты информации и проведение оценки безопасности выбранного средства защиты информации.

Для выполнения поставленной цели в работе были сформулированы **следующие задачи:**

– привести предпосылки использования аппаратно-программных средств обеспечения информационной безопасности;

– проанализировать методы оценки соответствия средств защиты информации;

– провести оценку уровня обеспечения безопасности аппаратно-программного комплекса межсетевого экранирования.

Область исследования. Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 «Технология приборостроения».

Теоретическая и методологическая основа исследования

В основу работы легли работы белорусских и зарубежных ученых по проведению оценки безопасности аппаратно-программных средств защиты информации, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, предоставляемой производителями микроконтроллеров, технических нормативно-правовых актов, сведений из ресурсов Интернет, а также материалов научных изданий, конференций и семинаров.

Научная новизна и значимость полученных результатов работы заключается в проведении оценки безопасности аппаратно-программных средств защиты информации.

Основные положения, выносимые на защиту

Предпосылки использования аппаратно-программных средств обеспечения информационной безопасности.

Анализ методов оценки соответствия средств защиты информации.

Оценка уровня обеспечения безопасности аппаратно-программного комплекса межсетевого экранирования.

Теоретическая значимость: предложена подробная классификация основных угроз информационной безопасности. Приведены методы и средства обеспечения информационной безопасности. Выполнен анализ методов оценки соответствия средств защиты информации. Проведена оценка уровня обеспечения безопасности аппаратно-программного комплекса межсетевого экранирования.

Практическая значимость диссертации состоит в том, что предложенная процедура оценки безопасности аппаратно-программных средств защиты информации затрагивает требования технических нормативных правовых актов по обеспечению информационной безопасности и позволят проводить оценку для различных уязвимостей. Рассмотрены методы оценки соответствия средств защиты информации.

Апробация и внедрение результатов исследования

Результаты проделанной работы были использованы при проведении аттестации системы защиты информации Республиканской автоматизированной системы ведения централизованного банка данных документов об образовании, выданных учреждениями образования Республики Беларусь.

Результаты работы по теме диссертации были представлены на XVI международной научно-практической конференции «Вопросы современных научных исследований» (г. Омск, Российская Федерация, 2018 г.), X Международной научно-методическая конференции «Дистанционное обучение – образовательная среда XXI века» (г. Минск, Республика Беларусь, 2017 г.), V международной научно-практической конференции «Проблемы эффективности функционирования технических и информационных систем» (г. Санкт-Петербург, Российская Федерация, 2018 г.) и на II международной научно-практической конференции «*ADVANCED SCIENCE*» (г. Пенза, Российская Федерация, 2018 г.).

Отдельные положения диссертации могут быть использованы при преподавании дисциплин «Основы защиты информации и управление интеллектуальной собственностью», «Компьютерные сети и сетевая безопасность» и «Криптографическая защита информации в ТК».

Публикации

Основные положение диссертации и результаты исследования изложены в шести опубликованных работах общим объемом 12 страниц.

Структура и объем работы

Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений. Объем основного текста диссертации − 55 страниц. Работа содержит 8 таблиц, 12 рисунков. Библиографический список включает 51 наименование.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы оценки безопасности аппаратно-программных средств защиты информации, указаны основные направления исследований, проводимых в мире по данной тематике, а также описано обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы цель и задачи диссертации, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также структура и объем диссертации.

В первой главе был осуществлен анализ и выполнена классификация угроз информационной безопасности, методов и средств обеспечения информационной безопасности, по таким признакам как: природа возникновения, степень зависимости от действий человека и место возникновения угрозы (таблица 1).

Таблица 1 – Классификация угроз безопасности [1]

Угрозы	Степень зависимости от действий человека	Внешние	Внутренние
Естественные	Преднамеренные	Развитие технологий	
	Непреднамеренные	Стихийные бедствия	Отказ техники Технические сбои
Искусственные	Преднамеренные	Разработка ПО Угроза целостности Угроза доступности	Угроза конфиденциальности Угроза целостности Угроза доступности
	Непреднамеренные	Политические факторы Социальные факторы	Ошибки ПО

В рамках исследований по теме диссертации было изучены искусственные преднамеренные угрозы конфиденциальности, целостности и доступности информации [1].

Проанализированы существующие методы и средства защиты информации, которые подразделяются на четыре основные группы:

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

Рассмотрены сервисы безопасности, к которым относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование [1]. Установлено, что для защиты информации от несанкционированного доступа создается система разграничения доступа

пользователей к информации. Диспетчер доступа реализуется в виде аппаратно-программных механизмов и представлен на рисунке 1.

Установлено, что для защиты информации могут использоваться криптографические методы. На рисунке 2 продемонстрировано эффективное шифрование, реализованное путем сочетания симметричного и асимметричного методов [2].

Проведен обзор национальных нормативных актов в области информационной безопасности и сертификации средств защиты информации по требованиям безопасности информации. Проанализированы основные требования к проведению процедуры оценки безопасности аппаратно-программных средств защиты информации.

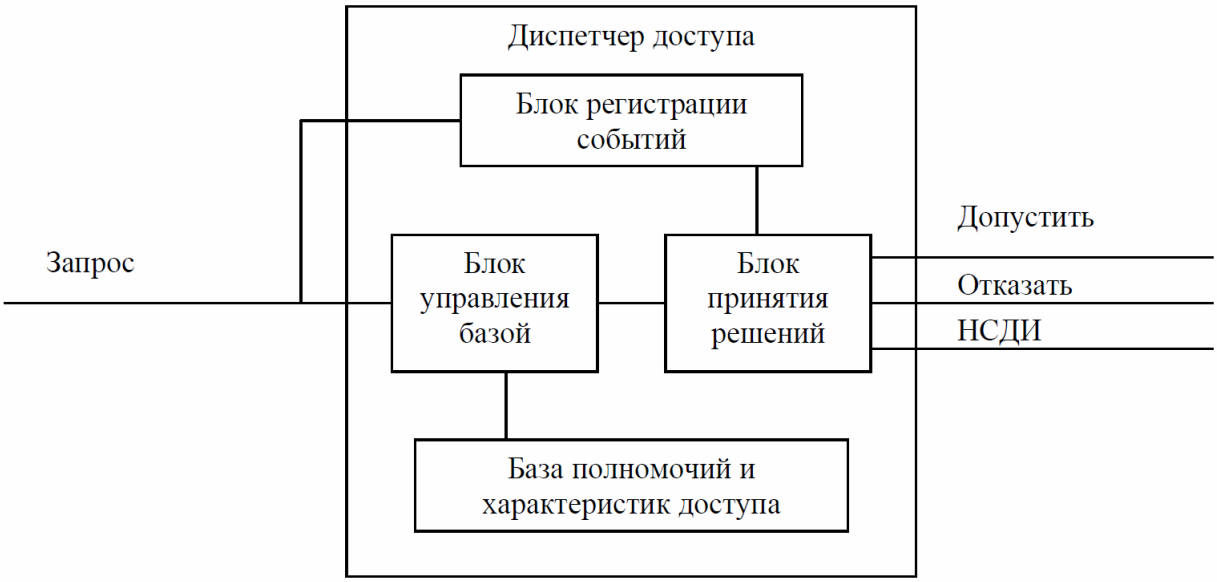

Рисунок 1 – Диспетчер доступа в виде аппаратно-программных механизмов

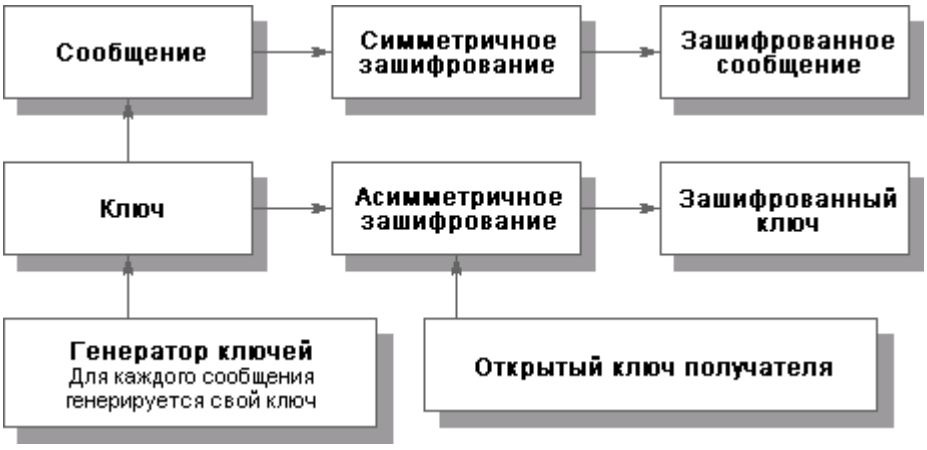

Рисунок 2 – Эффективное шифрование сообщения

Приведены обоснования потребности организаций в оценке безопасности средств защиты информации. Рассмотрены технические аспекты и основные причины возникновения проблем в области защиты информации, нормативно-методическое обеспечение создания и оценки средств защиты информации [3].

Во второй главе как один из методов прводения оценки безопасности аппаратно-программных средств защиты информации проанализирован метод оценки соответсвия требованиям технических нормативных правовых актов [4, 5].

Изучен функциональный подход к оценке соответствия средств защиты информации установленным требованиям. Схема функционального подхода представлена на рисунке 3.

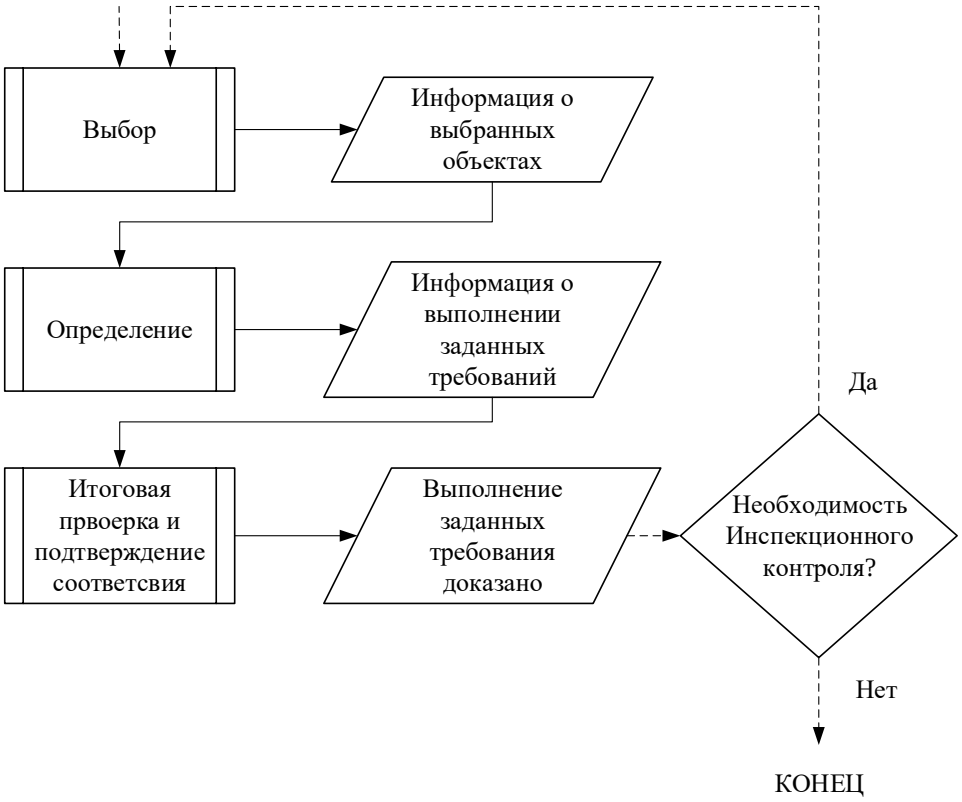

Рисунок 3. – Функциональный подход оценки соответствия

Определены виды процедур оценки соответствия средств защиты информации. Основными видами процедур оценки соответствия средств защиты информации являются [4]:

сертификация;

испытания;

аттестация;

тестирование;

аудит;

анализ рисков.

Проанализированы общие критерии защищённости информационных технологий. Безопасность в общих критериях рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

– определение назначения, условий применения, целей и требований безопасности;

– проектирование и разработка;

– испытания, оценка и сертификация;

– внедрение и эксплуатация.

Третья глава посвящена проведению оценки соответствия аппаратно-программного комплекса межсетевого экранирования «Цитадель на базе Sophos UTM 9» требованиям, изложенным в технических нормативных правовых актах. По результатам анализа методики испытаний межсетевых экранов, была осуществлена оценка безопасности аппаратно-программного комплекса межсетевого экранирования «Цитадель на базе *Sophos UTM* 9» путем проведения сертификационных испытаний. В ходе проведения испытаний были проведены следующие проверки:

– проверка механизмов фильтрации данных и трансляции адресов;

– проверка механизмов идентификации и аутентификации администраторов;

– проверка механизмов контроля целостности.

С целью проверки аппаратно-программного комплекса межсетевого экранирования «Цитадель на базе *Sophos UTM* 9» на наличие уязвимостей, была проведена проверка с использованием средства контроля защищенности «*Maxpatrol Server Pentest*» [6]. По результатам проверки уязвимостей обнаружено не было.

По результатам проведения испытаний было принято решение о соответствии аппаратно-программный комплекс межсетевого экранирования «Цитадель на базе *Sophos UTM* 9» требованиям действующих ТНПА.

ЗАКЛЮЧЕНИЕ

При работе над магистерской диссертацией были тщательно рассмотрены, изучены и проанализированы современные методы и способы оценки безопасности аппаратно-программных средств защиты информации.

На первом этапе выполнения данной работы был проведен анализ основных угроз информационной безопасности выявил необходимость в проведение различных мероприятий, направленных на обеспечение защиты информации, в том числе используя аппаратно-программные средства защиты информации. В ходе анализа различных средств защиты информации было сделано заключение о необходимости использования комплексной системы защиты информации, включающей в себя правовые, организационные и технические меры обеспечения информационной безопасности. На основании анализа национальных нормативных актов в области информационной безопасности, средства защиты информации, используемые в системах защиты информации информационных систем, подлежат оценке соответствия требованиям технических нормативных правовых актов. Таким образом оценка безопасности аппаратно-программных средств защиты информации осуществляется путем проведения испытаний и подтверждения соответствия установленным требованиям.

На втором этапе выполнения диссертационной работы выполненный анализ методов оценки соответствия средств защиты информации требованиям, изложенным в технических нормативно-правовых актах. В соответствии с требованиями ТНПА и проведенным обзором методов оценки соответствия было установлено, что оценка безопасности средств защиты информации осуществляется путем проведения сертификационных испытаний с дальнейшей выдачей сертификата соответствия. В ходе анализа был выбран базис сертификационных испытаний СЗИ, который позволяет определить факторы, связанные со временем, стоимостью и полнотой испытаний СЗИ [4].

На третьем этапе выполнения работы осуществлялась оценка безопасности аппаратно-программного комплекса межсетевого экранирования «Цитадель на базе *Sophos UTM* 9». По результатам проведения испытаний было принято решение о соответствии аппаратно-программного комплексf межсетевого экранирования «Цитадель на базе *Sophos UTM* 9» требованиям действующих ТНПА.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Богатко, М.П. Угрозы информационной безопасности при получении дистанционного образования / М.П. Богатко, И.Н. Богатко, Д.А. Качан // Дистанционное обучение – образовательная среда XXI века. Сборник материалов X Международной научно-методической конференции (г. Минск, Республика Беларусь, 19 ноября, 2017 г.) / Минск, БГУИР, 2018. – С. 182–183.

[2] Фисунов, А.В. Обзор мер безопасности в системах электронного документооборота / А.В. Фисунов, М.П. Богатко, В.В. Щеголев // Вопросы современных научных исследований. Сборник материалов XVI международной научно-практической конференции (г. Омск, Российская Федерация, 19 января, 2018 г.) Научный центр «Орка» – Омск, 2018. – С. 203–206.

[3] Богатко, М.П. Анализ комплексных систем защиты информации от несанкционированного доступа / М.П. Богатко, А.В. Фисунов, В.В. Щеголев // Вопросы современных научных исследований. Сборник материалов XVI международной научно-практической конференции (г. Омск, Российская Федерация, 19 января, 2018 г.) Научный центр «Орка» – Омск, 2018. – С. 135–139.

[4] Богатко, М. П. Основы оценки соответствия средств защиты информации требованиям, изложенным в технических нормативно-правовых актах / М.П. Богатко, А.В. Фисунов, В.В. Щеголев. // Современные тенденции в науке. Сборник материалов II международной научно-практической конференции (г. Самара, Российская Федерация, 20 января, 2018 г.). – С. 164–168.

[5] Щеголев, В.В. Концепция к постановке задачи принятия решений и выбору альтернатив при создании сложных технических систем / В.В. Щеголев, А.В.Фисунов, М.П. Богатко М.П. // *ADVANCED SCIENCE*. Сборник материалов II международной научно-практической конференции (Россия, Пенза, 17 января 2018 г.). – С. 160–161.

[6] Щеголев, В.В. Обзор программных комплексов расчета надежности технических систем / В.В. Щеголев, А.В. Фисунов, М.П. Богатко // Проблемы эффективности функционирования технических и информационных систем. Сборник материалов V международной научно-практической конференции (Россия, Санкт-Петербург, 16 января 2018 г.)) / ФГБОУ ВО «ВГЛТУ», Воронеж. 2015. –С. 157–158.

РЭЗЮМЭ

Багатка Максім Паўлавіч

Ключавыя словы: інфармацыйная бяспека, ацэнка, методыка, міжсеткавы экран..

Мэта работы: аналіз карыстаных методык і мадэляў пры правядзенні ацэнкі бяспекі апаратна-праграмных сродкаў абароны інфармацыі і правядзенне ацэнкі бяспекі абранага сродку абароны інфармацыі.

Атрыманыя вынікі і іх навізна: праведзены аналіз асноўных пагроз інфармацыйнай бяспекі выявіў патрэбу ў правядзенне розных імпрэз, скіраваных на забеспячэнне абароны інфармацыі, у тым ліку скарыстаючы апаратна-праграмныя сродкі абароны інфармацыі. На падставе аналізу нацыянальных нарматыўных актаў у вобласці інфармацыйнай бяспекі, сродку абароны інфармацыі, што выкарыстоўваюцца ў сістэмах абароны інфармацыі інфармацыйных сістэм, падлягаюць ацэнцы адпаведнасці вымогам тэхнічных нарматыўных праўных актаў.

Выкананы аналіз метадаў ацэнкі адпаведнасці сродкаў абароны інфармацыі вымогам, выкладзеным у тэхнічных нарматыўна-праўных актах. У адпаведнасці з вымогамі ТНПА і праведзеным аглядам метадаў ацэнкі адпаведнасці ўсталявана, што ацэнка бяспекі сродкаў абароны інфармацыі ўжыццяўляецца шляхам правядзення сертыфікацыйных выпрабаванняў з далейшай выдачай сертыфіката адпаведнасці. Абраны базіс сертыфікацыйных выпрабаванняў СЗИ, які дазваляе вызначыць фактары, злучаныя з часам, коштам і поўнасцю выпрабаванняў СЗИ.

Праведзена ацэнка бяспекі апаратна-праграмнага комплексу міжсеткавага экранавання «Цытадэль на базе *Sophos UTM* 9». Па выніках правядзення выпрабаванняў прыняты развязак пра адпаведнасць апаратна-праграмнага комплекс міжсеткавага экранавання «Цытадэль на базе *Sophos UTM* 9» вымогам дзейных ТНПА.

Ступень выкарыстання: вынікі ўкаранёны на кафедры ПІКС ў навучальны працэс.

Вобласць ужывання: сертыфікацыя сродкаў абароны інфармацыі, атэстацыя сістэм абароны інфармацыі.

РЕЗЮМЕ

Богатко Максим Павлович

***Ключевые слова*:** информационная безопасность, оценка, методика, межсетевой экран.

***Цель работы*:** анализ используемых методик и моделей при проведении оценки безопасности аппаратно-программных средств защиты информации и проведение оценки безопасности выбранного средства защиты информации.

***Полученные результаты и их новизна*:** проведен анализ основных угроз информационной безопасности выявил необходимость в проведение различных мероприятий, направленных на обеспечение защиты информации, в том числе используя аппаратно-программные средства защиты информации. На основании анализа национальных нормативных актов в области информационной безопасности, средства защиты информации, используемые в системах защиты информации информационных систем, подлежат оценке соответствия требованиям технических нормативных правовых актов.

Выполнен анализ методов оценки соответствия средств защиты информации требованиям, изложенным в технических нормативно-правовых актах. В соответствии с требованиями ТНПА и проведенным обзором методов оценки соответствия установлено, что оценка безопасности средств защиты информации осуществляется путем проведения сертификационных испытаний с дальнейшей выдачей сертификата соответствия. Выбран базис сертификационных испытаний СЗИ, который позволяет определить факторы, связанные со временем, стоимостью и полнотой испытаний СЗИ.

Проведена оценка безопасности аппаратно-программного комплекса межсетевого экранирования «Цитадель на базе *Sophos UTM* 9». По результатам проведения испытаний принято решение о соответствии аппаратно-программного комплекс межсетевого экранирования «Цитадель на базе *Sophos UTM* 9» требованиям действующих ТНПА.

***Степень использования*:** результаты внедрены на кафедре ПИКС в учебный процесс

***Область применения*:** сертификация средств защиты информации, аттестация систем защиты информации.

SUMMARY

Bogatko Maksim Pavlovich

Keywords: information security, assessment, methodology, firewall.

The object of study: analysis of the methods and models used in assessing the security of hardware and software security tools and conducting an assessment of the security of the chosen information protection means.

The results and novelty: The analysis of the main threats to information security has revealed the need to conduct various activities aimed at ensuring the protection of information, including using hardware and software to protect information. Based on the analysis of national regulations in the field of information security, information protection tools used in information systems for information systems protection are subject to assessment of compliance with the requirements of technical regulatory legal acts.

The analysis of methods for assessing the compliance of information security means with the requirements set out in technical regulations. In accordance with the requirements of the TNPA and the review of the methods for assessing compliance, it was established that an assessment of the security of information protection means is carried out by conducting certification tests with further issuance of a certificate of conformity. The basis of certification tests of GIS is chosen, which allows to determine the factors associated with the time, cost and completeness of GIS tests.

The security of the hardware-software inter-network shielding system «Citadel based on Sophos UTM 9» was evaluated. Based on the results of testing, a decision was made on the compliance of the hardware and software firewall system Citadel based on Sophos UTM 9 to the requirements of the current TNPA.

Degree of use: results are implemented in the Department of PICS in the educational process.

Sphere of application: certification of information security means, attestation of information security systems.