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

УДК 004.056.53

На правах рукописи

КОЛЕСНИКОВИЧ
Денис Сергеевич

АЛГОРИТМ ОПТИМАЛЬНОГО ВЫБОРА ЭФФЕКТИВНОГО ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

АВТОРЕФЕРАТ
магистерской диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

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

Научный руководитель: **ГОНОВ Александр Николаевич,**
кандидат технических наук, доцент, доцент кафедры проектирования информационно компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ПОЛУБОК Владислав Анатольевич,**
кандидат технических наук, доцент, заведующий кафедрой микропроцессорных систем и сетей института информационных технологий «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «26» января 2017 г. года в $11^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

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

СОГЛАСОВАНО:
Научный руководитель А.Н. Гонов
кандидат технических наук,
доцент

ВВЕДЕНИЕ

Жизнь современного общества немыслима без современных информационных технологий. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии. Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.)

Учитывая важность систем защиты информации (СЗИ), особое внимание целесообразно уделить их оптимальному выбору. Несмотря на современный уровень развития СЗИ, обеспечить безопасность информации каждого человека по-прежнему сложно.

На настоящий момент существует достаточно большое количество работ отечественных исследователей, рассматривающих влияние СЗИ (Грибунин В.Г., Чудовский В.Н., Домарев В.В., Щеглов А.Ю.) Заслуживают внимания работы J. Garstka, S. Northcutt, J. Novak. и других зарубежных авторов.

В исследованиях, представленных в научно-технической литературе, приведены результаты, подтверждающие огромное значение СЗИ в современном обществе. Однако вопросам оптимального выбора СЗИ не уделяется должного внимания. Среди множества существующих на данный момент СЗИ очень сложно выбрать ту, которая будет максимально эффективной в той или иной ситуации. В этой связи исследования по теме диссертации, направленные на правильный выбор нужной СЗИ, являются актуальными.

Выражаю благодарность за оказанную помощь в ходе подготовки диссертационной работы своему научному руководителю, кандидату технических наук, доценту кафедры ПИКС, Гонову Александру Николаевичу, а также за высококвалифицированные консультации по возникающим вопросам кандидату технических наук, доценту кафедры ПИКС, Алексееву Виктору Федоровичу.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Актуальность темы диссертационной работы обусловлена объективной необходимостью разработки корректных алгоритмов оптимального выбора эффективного варианта СЗИ от несанкционированного доступа, моделей защищенности, эффективных методик синтеза СЗИ, обеспечивающих эффективный выбор нужной системы защиты информации для потребителя.

Степень разработанности проблемы

В современных исследованиях, представленных в научно-технической литературе, приведены результаты экспериментальных исследований СЗИ. Результаты оказываются зачастую не применимыми в силу их разобщенно-

сти, и не позволяют пользователю сделать выбор в пользу нужной СЗИ.

Цель и задачи исследования

Целью диссертации является разработка теоретических основ для моделирования алгоритма оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа.

Для достижения поставленной цели в работе необходимо было решить следующие конкретные задачи:

1. Провести анализ моделей защищенности автоматизированной системы от несанкционированного доступа, учитывающих зависимость рисков от длительности инцидентов информационной безопасности (ИБ).

2. Разработать методику синтеза системы защиты информации от несанкционированного доступа для автоматизированных систем с учетом менеджмента инцидентов информационной безопасности

3. Разработать алгоритм оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа.

Область исследования

Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 81 01 «Компьютерные технологии проектирования электронных систем»

Теоретическая и методологическая основа исследования

В основу работы легли работы белорусских и зарубежных ученых по изучению систем защиты информации от несанкционированного доступа, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

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

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в разработке алгоритма оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа.

Теоретическая часть работы заключается в предложении подхода к нахождению вероятностей преднамеренных атак на основе анализа потенциала нарушителя, тогда как в большинстве известных работ вероятность атак находится исходя из предположения о пуассоновском законе распределения их плотности. Предложенный подход позволяет учесть больше априорных сведений о нарушителе, что дает возможность более точно определить вероятности атак и соответствующие риски.

Практическая значимость диссертации состоит в разработке модели защищенности автоматизированной системы от несанкционированного доступа с учетом зависимости рисков от длительности инцидентов информационной безопасности.

Основные положения, выносимые на защиту

1. Систематизация моделей защищенности автоматизированной системы от несанкционированного доступа, основанная на зависимости рисков от длительности инцидентов ИБ, позволяющая сделать вывод, что ни один из подходов в полной мере не отвечает предъявляемым требованиям.

2. Разработка методики синтеза СЗИ автоматизированной системы от несанкционированного доступа с учетом менеджмента инцидентов информационной безопасности, позволяющей определить вероятность предотвращения угрозы.

3. Разработка алгоритма оптимального выбора эффективного варианта СЗИ от несанкционированного доступа, позволяющего выбрать нужную СЗИ для решения поставленной задачи.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на республиканской конференции УО «Белорусский государственный университет информатики и радиоэлектроники».

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 6 печатных работах научной конференции.

Общий объем публикаций по теме диссертации составляет 6 листов.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений

В первой главе проведен анализ существующих подходов к моделированию и эффектному построению системы защиты информации от несанкционированного доступа. Показана эффективность системы защиты информации от несанкционированного доступа. Сформулированы задачи исследования, решаемые в диссертационной работе.

Во второй главе представлена модель защищенности автоматизированной системы от несанкционированного доступа, с учетом зависимости рисков от длительности инцидентов информационной безопасности. Проведен обзор известных работ по моделированию и оптимизации построения системы защиты информации, моделей защищенности автоматизированных

систем. Разработана модель защищенности автоматизированных систем с учетом разнотипности ущерба, стоимости, времени восстановления, вероятности преднамеренных атак. Рассмотрен баланс между стоимостью средств защиты информации и средств восстановления после инцидентов информационной безопасности.

Третья глава посвящена методике синтеза системы защиты информации от несанкционированного для автоматизированных систем с учетом менеджмента инцидентов информационной безопасности. Рассмотрены особенности проектирования систем защиты информации и выбор ее структуры.

В четвертой главе рассмотрен алгоритм оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа. Поставлена задача многокритериального оптимального выбора системы зашиты информации от несанкционированного доступа. Проведено сравнение эффективности систем защиты информации, созданных с применением различных подходов.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

В приложении представлены публикации автора и акт внедрения.

Общий объем диссертационной работы составляет 76 страниц. Из них 55 страниц основного текста, 16 иллюстраций на 16 страницах, 11 таблиц на 12 страницах, библиографический список из 51 наименования на 4 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы исследований, сформулирована цель работы, обоснованы научная и практическая значимость результатов, представлены основные положения, выносимые на защиту.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе выявлены источники требований по ИБ, разновидности тайн, которые защищать обязательно с точки зрения действующего законодательства. В АС, в которых обрабатывается информация, сведения которой содержат данные тайны, СЗИ должна быть реализована обязательно и соответствовать требованиям руководящим документов в этой области. В АС критически важных сегментов информационной инфраструктуры также необходима реализация СЗИ, в независимости от того, содержит ли обрабатываемая в них информация какую-либо тайну.

Частные показатели эффективности СЗИ можно разделить на внешние и внутренние.

К внешним ЧПЭ СЗИ отнесены обеспечиваемая защищенность АС, снижение риска ИБ, стоимость СЗИ, сроки ее создания, используемые СЗИ ресурсы и т.п..

К внутренним ЧПЭ СЗИ отнесены наличие и уровень сертификатов соответствия по требованиям ИБ у элементов СЗИ, однородность средств защиты информации (СрЗИ), масштабируемость, сопровождаемость, простота освоения СрЗИ и т.п.

При проектировании СЗИ все вышеприведенные ЧПЭ должны тем или иным образом учитываться. При решении оптимизационных задач по синтезу СЗИ многие из ЧПЭ могут быть вынесены в ограничения.

В общем случае задача проектирования оптимальной по критерию стоимости СЗИ, удовлетворяющей требованиям заказчика, может быть записана в виде:

$$C_{\Sigma} = \min C_{\Sigma k} | R_i \le R^*_i, \qquad (1.1)$$

где C_{Σ} – суммарная стоимость СЗИ с учетом мер восстановления после инцидента: $C_{\Sigma} = \sum_i C_{\text{СрЗИ}} + \sum_j d_j$;

$k=1,\dots K$ – варианты построения СЗИ;*

i – текущий номер ресурса (объединять риски для различных ресурсов не всегда оправданно).

Возможна и несколько другая постановка задачи, когда на суммарную стоимость СЗИ накладываются ограничения $C_{\Sigma} \le C^*_{\Sigma}$. Тогда можно поставить задачу минимизации риска (например, минимизацию среднего риска, рассматриваемого как матожидание потерь) и сравнивать результат с требуемым результатом. Однако в такой постановке целесообразно рассматривать задачу в случае, когда количество различных ресурсов невелико, так как зачастую сумма ущербов не имеет смысла (например, сложно объединить ущерб от атаки на Интернет-магазин организации и на используемую в ней программу бухучета).

Во второй главе разрабатывается модель защищенности автоматизированной системы от несанкционированного доступа, учитывающая зависимость рисков от длительности инцидентов ИБ.

Анализ подходов к моделированию СЗИ, в том числе, моделей, построенных на основе теории графов, автоматов, сетей Петри, вероятностных моделей, выполнялся по возможности расчета таких параметров, как вероятностей преодоления рубежей защиты, времени преодоления рубежей защиты и времени обнаружения воздействия, рисков ИБ.

С целью выявления недостатков известных моделей защищенности АС (с полным перекрытием, с частичным перекрытием) выполнен их анализ. Показано, что они не учитывают среды безопасности АС, структуры построения АС и вида обрабатываемой информации.

Отмечено, что остаточный риск ИБ зависит не только от СЗИ, но и от системы менеджмента инцидентов ИБ. Рассмотрена задача нахождения ба-

ланса между ресурсами, выделяемыми на СЗИ, и на систему восстановления после инцидентов ИБ.

На рисунке 1 через $Cc_pзu_i$ обозначена стоимость механизмов защиты, парирующих атаки, через d_i – стоимость механизмов защиты, обеспечивающих восстановление после инцидентов. $U_1,\ldots,U_L$ – набор ресурсов АС S, на которые производятся атаки.

При этом на один ресурс может быть реализовано несколько атак. Точно также как и одна атака может быть направлена на несколько ресурсов.

Риск *Ri* зависит от времени нахождения в небезопасном состоянии АС $\Delta t_{восст}$.

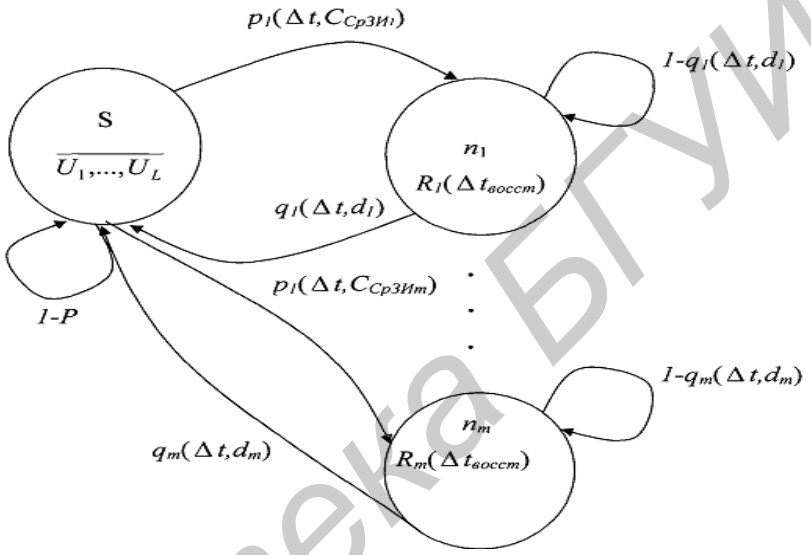

Рисунок 1 – Модель защищенности АС, учитывающая временные стоимостные факторы, а также тип ущерба

Вероятности p_i и q_i (успешной атаки и возвращения в безопасное состояние, соответственно) зависят от интервала времени, на котором они рассматриваются.

Вероятность p_i , кроме того, зависит от стоимости СрЗИ, а интервал времени нахождения в небезопасном состоянии АС зависит от стоимости средств восстановления d_i. Качественно эта зависимость изображена на рисунке 2.

Как видно из рисунка 2 вероятности p_i и q_i с увеличением интервала времени наблюдения стремятся к 1. При этом с увеличением стоимости СрЗИ вероятность перехода в небезопасное состояние уменьшается. С увеличением стоимости средств восстановления вероятность перехода в безопасное состояние увеличивается. Если не решать задачу восстановления, то АС всегда будет в небезопасном состоянии. С увеличением расходов на мероприятия восстановления время нахождения в небезопасном состоянии уменьшается и достигает некоторого фиксированного значения, для каждого ресурса АС связанного тем или иным образом с физическими ограничениями (например, время перезагрузки системы или переустановки жесткого

диска или отработки антивирусного средства).

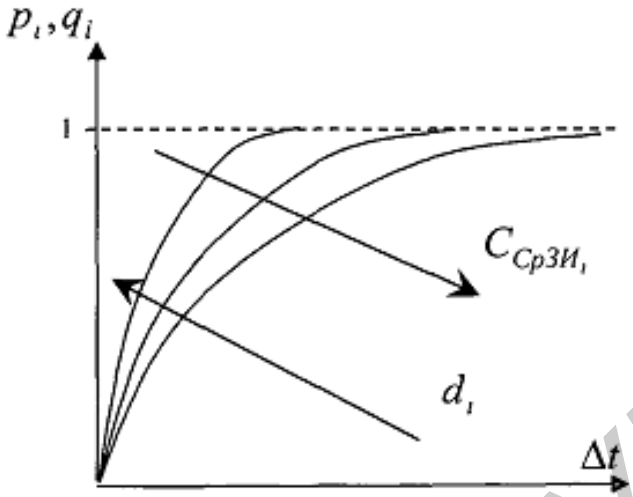

Рисунок 2 – Качественная зависимость между стоимостью и вероятностно-временными характеристиками

Чтобы нарушитель использовал уязвимость, ее необходимо сначала идентифицировать, а затем использовать.

При анализе потенциала нападения, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

1) идентификация:

– время, затрачиваемое на идентификацию уязвимости;

– техническую компетентность специалиста;

– знание проекта и порядка функционирования АС;

– доступ к АС;

– аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для анализа;

2) использование:

– время, затрачиваемое на использование уязвимости;

– техническая компетентность специалиста;

– знание проекта и порядка функционирования АС;

– доступ к АС;

– аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для использования уязвимости.

Во многих случаях эти факторы не являются независимыми и могут в различной степени заменять друг друга. Например, компетентность или аппаратные средства/программное обеспечение могут быть заменой времени.

В третьей главе разработана методика синтеза системы защиты информации автоматизированной системы от несанкционированного доступа с учетом менеджмента инцидентов информационной безопасности.

В целом шаги методики описаны ниже.

1. Общее описание архитектуры АС, ее составных элементов, системы

защиты информации и правил политики безопасности. Анализ рисков с учетом их длительности, остаточных рисков и потенциала нападения нарушителя.

2. Формализация описания системы защиты информации, разработка формальных правил разграничения доступа

3. Формулирование требований, которым должна удовлетворять СЗИ и подсистема менеджмента инцидентов ИБ для качественного выполнения возложенных на них функций. Выбор ЧПЭ СЗИ и подсистемы менеджмента инцидентов ИБ.

4. Выбор частных показателей качества СрЗИ и средств восстановления АС, поиск имеющихся на рынке СрЗИ, удовлетворяющих требованиям, и определение необходимости создания новых. Анализ существующих проектов СЗИ и менеджмента ИБ.

5. Выбор эффективных вариантов СЗИ и восстановления АС на основе алгоритма многокритериальной потоковой оптимизации.

Отличие предлагаемой методики от известных методик синтеза СЗИ заключается в том, что в ней дополнительно учитываются:

– результаты анализа рисков, причем значение рисков считается увеличивающимся с увеличением времени нахождения АС в небезопасном состоянии;

– взаимосвязь остаточного риска со стоимостью используемых средств защиты информации и организационно-технических мероприятий менеджмента инцидентов ИБ;

– баланс стоимости между стоимостью средств защиты информации и мер по восстановлению после инцидентов информационной безопасности.

Рассмотрены все новые предлагаемые шаги методики, подробно рассмотрены вопросы менеджмента инцидентов ИБ. Последний шаг методики описан в главе 4.

В четвертой главе разработан алгоритм оптимального выбора СЗИ на основе многокритериального потокового ранжирования, заключающийся в следующем.

Подготовка исходных данных. Выбор структуры СЗИ. На данном этапе организаторами экспертизы определяются границы области, в которой будет осуществляться поиск, анализ завершенных работ и обоснование параметров типовой СЗИ. Устанавливается тип АС, в которой будет применена СЗИ, режим обработки информации, ее гриф конфиденциальности, полномочия пользователей. Выбирается структура СЗИ на основе дерева решений.

Из различных источников осуществляется сбор информации об успешно завершенных проектах по созданию СЗИ. На данном этапе к успешным проектам относят работы, результаты которых соответствуют техническому заданию, выполнены в первоначально установленные сроки и объемы ассигнований.

Исходя из цели обоснования параметров типовой СЗИ, организаторы экспертизы формируют набор критериев для выбора оптимальной по пара-

метрам СЗИ. Для каждого из критериев определяется способ получения оценок параметров СЗИ, при необходимости разрабатываются соответствующие вербально-числовые шкалы.

Оценка параметров типовых СЗИ. Группа экспертов оценивает каждую СЗИ по набору критериев. Кроме самих СЗИ эксперты оценивают относительную важность критериев. В результате обобщения экспертных оценок вычисляются коэффициенты относительной важности критериев.

Решение задачи многокритериального потокового ранжирования.

Совокупность СЗИ преобразовывается в упорядоченную последовательность согласно оценкам по набору критериев. Для обеспечения наилучшего восприятия и анализа результатов ранжирования, последовательность выдается экспертам в виде графической диаграммы.

Анализ и экспертиза результатов. На данном этапе проводится коллективное обсуждение результатов упорядочения СЗИ. В случае наличия существенных расхождений в предпочтениях экспертов проводится уточнение оценок, повторное ранжирование и обсуждение полученных результатов.

Если эксперты согласны с результатами ранжирования СЗИ, то наиболее предпочтительная из них принимается в качестве типовой СЗИ.

Алгоритм многокритериального потокового ранжирования состоит из следующих шагов:

– выбор типа функций предпочтения и задание их параметров по каждому из критериев;

– определение матриц парных сравнений проектов по созданию СЗИ НСД по каждому из критериев;

– расчет исходящих потоков;

– расчет входящих потоков;

– расчет суммарных потоков;

– формирование результирующего упорядочения проектов.

Таким образом, учет рисков и менеджмента инцидентами ИБ позволили существенно снизить общий ущерб, создать более эффективную по обобщенному показателю эффективности СЗИ.

После наступления инцидента ИБ собственник АС вынужден тратить дополнительные ресурсы на ликвидацию его последствий. Это делает учет менеджмента инцидентов ИБ при проектировании СЗИ еще более актуальным.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Модель защищенности АС от несанкционированного доступа. Эта модель отличается от существующих учетом менеджмента инцидентов информационной безопасности. Чем больше внимания уделяется этому аспекту,

тем меньше время нахождения АС в небезопасном состоянии, а, следовательно, меньше ущерб от инцидентов ИБ. Другое отличие разработанной модели состоит в отказе от вероятностных подходов к моделированию преднамеренных атак в пользу учета потенциала нарушителя.

2. Методика синтеза системы защиты информации от несанкционированного доступа для автоматизированных систем с учетом менеджмента инцидентов информационной безопасности.

3. Алгоритм оптимального выбора эффективного варианта СЗИ от несанкционированного доступа на основе многокритериального потокового ранжирования. Применение данного метода позволяет оптимальным образом осуществить выбор проекта СЗИ среди известных.

Для рассматриваемой в работе АС увеличение обобщенного показателя эффективности СЗИ при применении предлагаемого подхода в сравнении с существующими составила: по сравнению с подходом без анализа рисков ИБ – в 2,43 раза; по сравнению с подходом с анализом рисков ИБ, но без учета менеджмента инцидентов ИБ – в 1,25 раз.

Цель диссертационной работы, заключающаяся в повышении эффективности СЗИ от несанкционированного доступа за счет менеджмента инцидентов ИБ и решения задачи многокритериального выбора СЗИ по разработанным ЧПЭ, достигнута.

Разработанные модели и методики могут применяться при проектировании СЗИ, при оценке ее эффективности, а также при оценке существующих СЗИ от несанкционированного доступа.

К направлениям дальнейших исследований можно отнести:

1) нахождение аналитических выражений для описания плотности распределения преднамеренных атак;

2) разработку подходов к оптимальному построению подсистемы менеджмента инцидентов ИБ;

3) нахождение аналитических зависимостей риска ИБ от времени длительности атаки;

4) нахождение рациональных критериев для решения задачи выбора оптимального варианта построения СЗИ методом многокритериального потокового ранжирования. Апробирование данной методики в ходе проектирования СЗИ в рамках выполнения ОКР.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Физические основы проектирования радиоэлектронных средств».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Богданович, А.А. Информационная безопасность мобильных сетей / А.А. Богданович, Д.С. Колесникович, А.Н. Гонов // Репозиторий БГУИР, 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/123456789/11459

2. Колесникович, Д.С. Оптимизация алгоритмов безопасности передачи голосовых данных / Д.С. Колесникович, А.Н. Гонов // Репозиторий БГУИР, 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/123456789/11460

3. Богданович, А.А. Основные концепции и методы защиты компьютерных сетей от несанкционированного доступа / Д.С. Колесникович, А.А. Богданович, А.Н. Гонов // Репозиторий БГУИР, 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/123456789/114

4. Богданович, А.А. Инновационные методы защиты информации от утечки по техническим каналам / Д.С. Колесникович, А.А. Богданович, А.Н. Гонов // Репозиторий УО «БГУИР», 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/123456789/11470

5. Колесникович, Д.С. Актуальные проблемы построения частных виртуальных сетей на базе IP / Д.С. Колесникович, А.Н. Гонов // Репозиторий БГУИР, 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/12345678/11489

6. Колесникович, Д.С. Основные критерии качества защиты информации / Д.С. Колесникович, А.А. Богданович, А.Н. Гонов // Репозиторий УО «БГУИР», 2017. – Режим доступа: https://libeldoc.bsuir.by/handle/123456/11564

РЭЗЮМЭ

Калесніковіч Дзяніс Сяргеевіч

Алгарытм аптымальнага выбару эфектыўнага варыянту сістэмы абароны інфармацыі ад несанкцыянаванага доступу

Ключавыя словы: сістэма абароны інфармацыі, несанкцыянаваны доступ.

Мэта працы: распрацоўка тэарэтычных асноў для мадэлявання алгарытму аптымальнага выбару эфектыўнага варыянту сістэмы абароны інфармацыі ад несанкцыянаванага доступу.

Атрыманыя вынікі і іх навізна: прапанаваны падыход да знаходжання верагоднасцяў наўмысных нападаў на аснове аналізу патэнцыялу парушальніка. Прадэманстравана, што рэшткавы рызыка ІБ залежыць не толькі ад эфектыўнасці сістэмы абароны інфармацыі, але і ад эфектыўнасці падсістэмы менеджменту інцыдэнтаў інфармацыйнай бяспекі. Распрацавана методыка сінтэзу сістэмы абароны інфармацыі, у якой улічаны новыя падыходы да ацэнкі рэшткавага рызыкі. Прапанаваны якасныя залежнасці рызыкі інфармацыйнай бяспекі ад часу працягласці атакі.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» у навучальны курс «Фізічныя асновы праектавання радыёэлектронных сродкаў».

Вобласць ужывання: магчымасць прымянення распрацаваных матэматычных мадэляў і методык пры абгрунтаванні праектаў па стварэнні сістэм абароны інфармацыі ад несанкцыянаванага доступу.

РЕЗЮМЕ

Колесникович Денис Сергеевич

Алгоритм оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа

***Ключевые слова*:** система защиты информации, несанкционированный доступ.

Цель работы: разработка теоретических основ для моделирования алгоритма оптимального выбора эффективного варианта системы защиты информации от несанкционированного доступа.

***Полученные результаты и их новизна*:** предложен подход к нахождению вероятностей преднамеренных атак на основе анализа потенциала нарушителя. Продемонстрировано, что остаточный риск ИБ зависит не только от эффективности системы защиты информации, но и от эффективности подсистемы менеджмента инцидентов информационной безопасности. Разработана методика синтеза системы защиты информации, в которой учтены новые подходы к оценке остаточного риска. Предложены качественные зависимости риска информационной безопасности от времени длительности атаки.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Физические основы проектирования радиоэлектронных средств».

***Область применения*:** возможность применения разработанных математических моделей и методик при обосновании проектов по созданию систем защиты информации от несанкционированного доступа.

SUMMARY

Kolesnikovich Denis Sergeevich

The algorithm of optimal choice of effective options to protect data from unauthorized access the system

Keywords: system of protection of information, unauthorized access.

***The object of study*:** To develop a theoretical framework for modeling algorithm, optimal choice of effective options to protect information systems from unauthorized access.

The results and their novelty: an approach to the determination of the probability of deliberate attacks on the basis of the analysis of the potential intruder. It is demonstrated that the residual risk of information security depends not only on the effectiveness of information security systems, but also on the effectiveness of the management subsystem of information security incidents. A method for the synthesis of information protection system, which takes into account new approaches to the assessment of the residual risk. Offer quality information security risk depending on the time duration of the attack.

***Degree of use*:** the results implemented in the educational process at the department of design information and computer systems educational institution "Belarusian State University of Informatics and Radio Electronics" in the course "Physical fundamentals of the design of radio-electronic means."

Sphere of application: the possibility of using the developed mathematical models and methods in the justification of projects on creation of information security systems from unauthorized access.