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

УДК 004.056.5

*На правах рукописи*

**КОРВЕЛЬ**
**Андрей Викторович**

# МЕТОДЫ И АЛГОРИТМЫ ВЫБОРА ОПТИМАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ

**АВТОРЕФЕРАТ**
диссертации на соискание степени
магистра техники и технологий

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

Минск 2019

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

Научный руководитель: **ГАЛУЗО Валерий Евгеньевич,**
кандидат технических наук, доцент, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **КИРИЧУК Андрей Викторович,**
заместитель директора представительства ЗАСО «Промтрансинвест» в г.Минске №3, магистр техники и технологии

Защита диссертации состоится «28» июня 2019 года в $9^{\underline{00}}$ 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. 408, тел. 293-20-80, e-mail: kafpiks@bsuir.by

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

# ВВЕДЕНИЕ

Одной из задач, с которой сталкивается любая организация, является проблема защиты деловой и частной информации, а также имущества и других объектов от действий злоумышленников. Бурное развитие информационных коммуникаций, расширение масштаба деловой активности и взаимодействия людей облегчает действия злоумышленников. Повышение ценности информации в современном мире делает задачу защиты еще более актуальной.

Защита информации и имущества осуществляется с использованием систем безопасности (СБ), которая имеет аппаратные и программные средства для осуществления задачи безопасности объектов защиты.

Под объектом защиты будем понимать некоторое имущество (физический объект защиты) или информацию (логический объект защиты). Безопасность объектов защиты означает такое состояние имущества, хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Объекты защиты в системе безопасности могут быть связаны между собой некоторыми функциональными связями. Примером может служить, например, связь соседних помещений для прохода людей. Объекты могут образовывать иерархические структуры. Доступ к внутренним объектам в иерархических структурах объектов защиты возможен только при осуществлении доступа к внешним объектам. В целом объекты защиты образуют некоторую сеть объектов. Они связанны между собой по одному или нескольким функциональным связям.

Следует отметить, что связи физических объектов между собой и с информационными объектами носят более сложный характер, чем связи информационных объектов между собой. Поэтому задача проектирования систем безопасности, включающих как физические, так и логические объекты, более сложная, чем проектирование с чисто информационными объектами.

Действия злоумышленников могут быть направлены на получение важной закрытой информации, на нанесение материального ущерба или ущерба репутации фирмы и др. Источник угрозы может исходить как извне, так и изнутри организации. Организация может быть размещена на нескольких удаленных друг от друга площадках, окруженных неконтролируемой ею потенциально враждебной средой (с точки зрения безопасности). Даже небольшая организация может включать сотни и более объектом защиты и десятки сотрудников и гостей; Достоверную оценку безопасности такой сложной системы на. этапе проектирования её общей структуры и основных функций можно получить только с использованием систем автоматизации проектирования (САПР).

Системы автоматизации проектирования системы безопасности (САПР СБ) сети объектов содержат инструменты для выбора и разработки аппаратуры, программного обеспечения и технической документации. Проектирование, установка и эксплуатация систем безопасности являются ответственными и дорогостоящими. Выбор неверных решений при проектировании системы может не позволить полностью решить задачу обеспечения безопасности. Поэтому для систем с высокими требованиями по безопасности стандартами предусмотрена разработка формальной модели управления доступом, включающей все субъекты и объекты данной системы. Должен проводиться анализ наличия побочных каналов утечек, и выявление элементов структуры СБ, критических с точки зрения защиты.

При работе системы безопасности ее основные параметры (объекты защиты, субъекты системы и права доступа субъектов к объектам) постоянно изменяются. Поэтому модель системы должна позволять использовать ее для анализа свойств и оценки качества обеспечения безопасности при управлении доступом в системе безопасности.

Однако известные модели безопасности ориентированы на использование в информационно-вычислительных системах, сложны для использования при оценке системы безопасности физических объектов, не всегда позволяют рассмотреть все возможные связи между элементами системы и варианты поведения субъектов системы. Поэтому актуальным является разработка адекватных моделей и методов для системы физической безопасности сети объектов.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования**

Главной целью любой системы защиты информации (СЗИ) является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта.

В современных условиях развития информационных технологий для коммерческих или государственных организаций, обязательно целесообразно предусмотреть создание методов и алгоритмов выбора оптимальной системы защиты информационной (СЗИ). Безусловно, еще на этапе проектирования информационной системы возникает вопрос эффективности средств защиты, созданной по тому или иному проекту. Решение задачи формального сравнения нескольких проектов для выбора наилучшего вызывает определенные сложности. Для оценки эффективности создаваемых СЗИ в Республике Беларусь

используются руководящие документы по техническому и экспортному контролю и ГОСТы.

Возникновение проблемы информационной безопасности во многом обусловлено широким распространением корпоративных информационно-вычислительных систем со слабо защищенным программно-техническим обеспечением. В этих условиях решение вопросов безопасности в информационной системе (ИС) реализуется с применением различных подходов, в том числе: автоматизированных инструментальных средств оценки рисков несанкционированного доступа (НСД) к информации (CRAMM, RiskWatch, COBRA и др.), автоматизированных средств тестирования, на наличие уязвимостей в информационной системе (ISS, SATAN, COPS и др.), автоматизированных средств проектирования систем защиты информации.

**Степень разработанности проблемы**

Данной проблеме посвящено значительное количество работ отечественных и зарубежных исследователей, среди которых В.А. Герасименко, В.В. Мельников, С.С. Корт, А.Г. Корченко, И.В. Котенко, М.В. Степашкин, В.И. Богданов, А.А. Малюк, Д.П. Зегжда, A. Moore, R. Ellison, R. Linger, S. Templeton, К Levitt, Xinming Ou, R.P. Lippman, O. Sheyner, J. Haines, S. Jha, J.Wing, S. Noel, S. Jajodia, M. Bishop, P. Ammann, B. Schneier и другие.

Существует множество современных международных и отечественных стандартов, нормативных документов в области информационной безопасности, рассматривающих вопросы оценки эффективности СЗИ или определяющих требования к её функциональности.

В этих документах, как правило, в качестве критерия эффективности используется наличие тех или иных средств защиты информации или требования к их параметрам и не учитывается, что имеются возможности преодоления данных средств за счет наличия в них тех или иных уязвимостей.

Несмотря на значительное количество исследований в этом направлении, отсутствует детальная информация о методах и алгоритмах выбора оптимального проекта СЗИ по критерию эффективности, учитывающему наличие уязвимостей и взаимосвязей между ними.

**Цель и задачи исследования**

Цель диссертационной работы состоит в разработке модели и методов для проектирования и управления работой системы безопасности объекта, а также методики анализа параметров обеспечения безопасности в этой системе.

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

1. Анализа возможных каналов угроз системы безопасности в информационной системе с целью разработки моделей и алгоритмов системы безопасности объекта, описывающей все взаимосвязи между компонентами СБ.

2. Разработка на основе предложенной модели методов анализа качества обеспечения безопасности в проектируемой системе безопасности.

3. Разработка на основе предложенной модели методов оценки качества поддержания безопасности в системе безопасности в ходе изменения параметров системы при управлении системой.

**Область исследования**

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 81 01-2012 специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

**Теоретическая и методологическая основа исследования**

Для решения поставленных задач использовались: методы теории вероятности и случайных процессов, методы дискретной математики, формальной логики, теория графов, математическое моделирование, теории, технологии и стандарты проектирования и функционирования, информационных систем и вычислительных сетей, теория и методы анализа эффективности и проектирования систем защиты информации.

Для оценки уровня защищенности, реализуемой средствами защиты, применялись формальные и неформальные методы обработки экспертных оценок, для выбора оптимального комплекса средств защиты» использовались методы оптимального проектирования и многоальтернативной оптимизации.

*Информационная база* исследования сформирована на основе литературы, открытой информации, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

**Научная новизна**

*Научная новизна* работы заключается в разработке методов анализа качества обеспечения безопасности в проектируемой системе, которые позволяют рассчитать доступность и недоступность всех объектов с учетом возможных каналов утечки, разработке методики проведения моделирования и выбора гарантированности обеспечения политики безопасности, базирующейся на анализе оценки качества поддержания безопасности в информационной системе в ходе изменения основных параметров системы (объектов защиты,

субъектов системы и прав доступа субъектов к объектам) при управлении ее работой.

*Теоретическая значимость* заключается в детальном анализе защищаемых информационных ресурсов и построении модели угроз, определении требований к системе защиты.

*Практическая значимость* диссертации заключается в том, что полученные результаты позволяют автоматизировать проектирование структуры системы безопасности, оценку параметров безопасности проектируемой системы и их соответствие поставленным требованиям. Предложенная модель и методы оценки качества поддержания политики безопасности упрощают и удешевляют проектирование и эксплуатацию систем безопасности.

**Основные положения, выносимые на защиту**

1. Сравнительный анализ возможных каналов угроз системы безопасности в информационной системе.
2. Модель и алгоритм оптимальной системы защиты информации в организации.
3. Методика проведения моделирования и выбора оптимального проекта.

**Апробация и внедрение результатов исследования**

Результаты исследований по теме диссертации докладывались и обсуждались на 54-й и 55-й научной конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Республика Беларусь, 2018 и 2019 годы), публиковались в международном научном журнале East European Scientific Journal (2019 год), в журнале «Евразийского Союза Ученых» (2019 год), в ежемесячном рецензируемом междисциплинарном журнале для ученых и практиков, для аспирантов и докторантов, для докторов наук и студентов «Scientific discussion» (2019 год).

По результатам исследований имеется акт внедрения (использования) результатов диссертации в учебном процессе в БГУИР.

**Публикации**

Основные положения диссертации и результаты исследования изложены в 8 печатных работах. В их числе 2 статьи в сборнике материалов научных конференций, 6 статей в рецензируемых научных журналах.

**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** дается терминология, основные понятия и общий обзор угроз безопасности, выполнен анализ систем защиты информации и их моделей, а также анализ алгоритмов, средств и методов защиты информации.

**Во второй главе** выполнена разработка модели и алгоритма оптимальной системы защиты информации в организации. была исследована модель ресурсов ИС. В рамках модели все ресурсы разделяются на программные, аппаратные и информационные. Анализ модели показал, что в ней не учитываются взаимосвязи ресурсов между собой и соответственно нельзя оценить, как воздействие на один из ресурсов ИС отражается на остальных ресурсах. Модель не рассматривает бизнес-процессы, поддерживаемые ИС, и их зависимость от ресурсов. Следовательно, для рассмотрения процессов защиты информации данная модель непригодна. Представлен алгоритм выбора оптимальных средств инженерно-технической защиты информации. Показаны подходы к разработке архитектуры программного комплекса и оценки адекватности модели реализации угрозы.

**В третьей главе** разработана методика проведения моделирования и выбора оптимального проекта. Показано, что на этапе сбора предварительной информации производится сбор информации о защищаемой информационной системе, о ее ресурсах, угрозах, требованиях владельца в системе защиты, потенциальных злоумышленниках и т.д. На этапе проектирования системы защиты создается ряд проектов, для которых определяются уязвимости и пути их использования, возможные пути атак злоумышленников на информационную систему.

**В четвертой главе** выполнено моделирование системы защиты информации на примере технического университета. Сделан анализ защищаемых информационных ресурсов и построение модели угроз, определены требований к системе защиты, разработан проект системы защиты информации ИС.

**В приложении** представлены публикации автора, акт внедрения, справка на антиплагиат и графический материал, иллюстрирующий основные результаты диссертационной работы.

Общий объем диссертационной работы составляет 91 страницы. Из них 63 страницы основного текста, 14 иллюстраций на 10 страницах, 4 таблицы на 2 страницах, библиографический список из 109 наименований на 9 страницах, список собственных публикаций соискателя из 6 наименований на 1 странице, 4 приложения на 24 страницах.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено состояние проблемы защиты деловой и частной информации, а также имущества и других объектов от действий злоумышленников, а также представлено обоснование актуальности темы диссертации.

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** выполнен анализ типовой структуры информационной системы и её системы защиты. На основании проведенного анализа было показано, что по структуре и принципам функционирования информационные системы типовых коммерческих и государственных организаций подобны корпоративным сетям и могут быть описаны соответствующими моделями.

Показано, что в процессе функционирования системы безопасности состав субъектов и объектов, права субъектов и связи объектов между собой могут динамически изменяться. При рассмотрении вопросов защиты исследования основывались на аксиоме, которая положена в основу американского стандарта по защите («Оранжевая книга») и предполагает, что все вопросы безопасности объектов определяются доступами субъектов к объектам.

Эта аксиома охватывает практически все известные способы нарушения безопасности в самых различных вариантах понимания безопасности. Следовательно, для рассмотрения вопросов безопасности и защиты объектов достаточно рассматривать множество объектов и доступ к ним субъектов.

Показано, что угрозы нарушения конфиденциальности (секретности) направлены на получении доступа к объектам (информации, имуществу) лицам, которые не должны иметь к ней доступ. Это происходит при несанкционированном доступе к некоторым закрытым объектам, который не связан с непосредственным их изменением или повреждением.

Установлено, что для надежной защиты организации от угроз необходимо ограничивать как физический, так и удаленный доступ к объектам защищаемой организации. Для защиты самой системы безопасности в сетевой среде необходимо защищать ее аппаратные средства, данные и линии передачи информации. Это подтверждает представленную аксиому о решающей роли контроля над доступом субъектов к объектам в вопросах обеспечения безопасности.

Во **второй главе** разработана модель ресурсов ИС, учитывающая взаимное влияние угроз для различных объектов. Модель разработана в виде неоднородной семантической сети.

В сети определены следующие типы связей между ресурсами:

– НК – связь типа «включает/хранит». Данный тип связи указывает, что исходный ресурс содержит другой ресурс, например, сервер содержит носители информации (жесткие диски) или носитель информации хранит информацию;

– РТ – связь типа «обрабатывает/передает». Данный тип связи указывает что исходный ресурс участвует в передаче или обработке зависимого. Обрабатывать и передавать можно, соответственно, только информацию;

– S – связь типа «поддерживает функционирование». Данный тип связи указывает, что от исходного ресурса зависит возможность функционирования зависимого ресурса.

Общий вид семантической сети, отображающей ресурсы ИС и бизнес-процессы, представлен на рисунке 1.

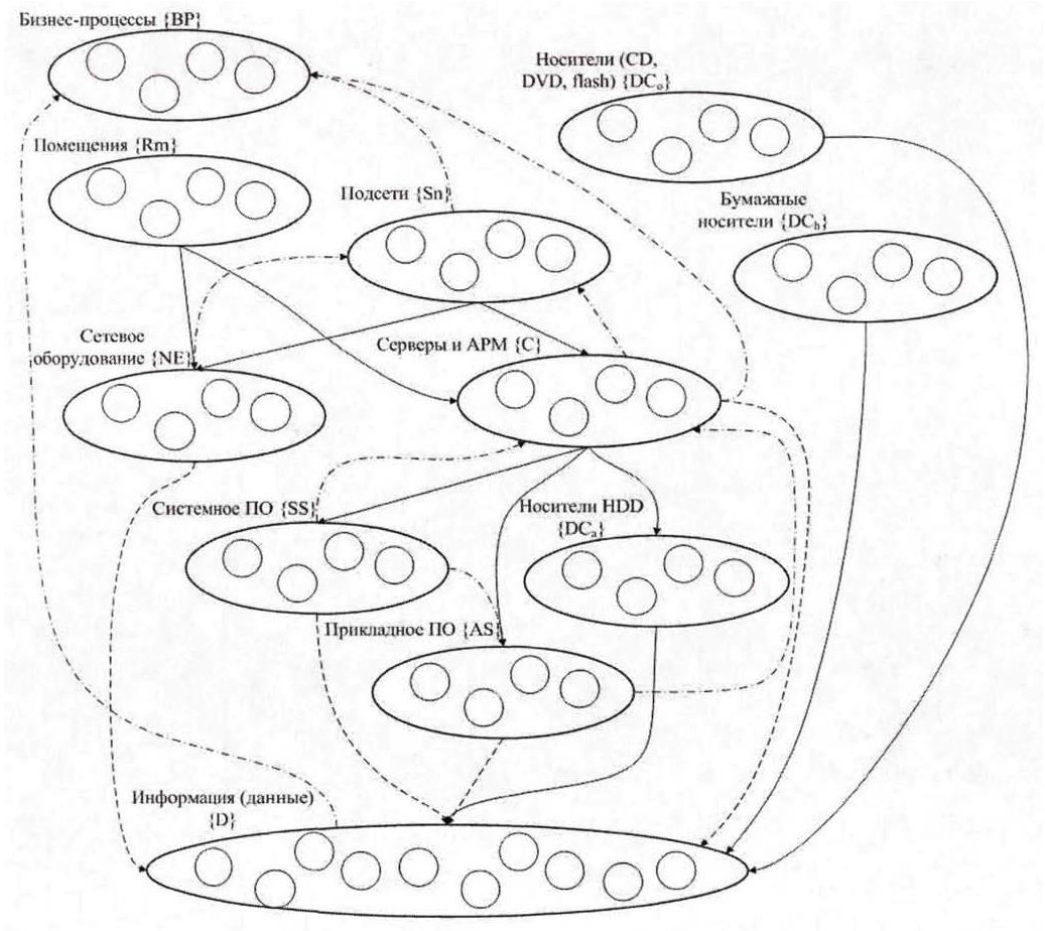


**Рисунок 1 – Модель ресурсов информационной системы**

Разработана иерархия моделей, включающая игровую модель поиска оптимального проекта СЗИ, игровые модели противостояния определенному типу злоумышленника и полумарковские модели реализации угроз.

Выполнено математическое описания игровой модели исследования оптимального проекта СЗИ, игровых моделей противостояния определенному

типу злоумышленника, полумарковских моделей реализации угроз, методики генерации дерева процесса реализации угроз, модели злоумышленника, методики проведения модельного эксперимента.

Разработана архитектура программного комплекса, включающая графический пользовательский интерфейс и библиотеку классов, реализующих разработанные алгоритмы моделирования.

Проведена оценка адекватности полумарковской модели реализации угрозы.

**В третьей главе** разработана методика проведения моделирования и выбора оптимального проекта.

Показано, что при принятии владельцем ИС решения на проведение исследования оптимальности предлагаемых проектов СЗИ создается рабочая группа (РГ), отвечающая за сбор исходных данных, подготовку проектов СЗИ, проведение моделирования и анализ результатов. Рабочая группа, в свою очередь использует следующую методику для проведения моделирования, включающую четыре основных этапа:

– этап сбора предварительной информации;

– этап проектирования системы защиты;

– этап моделирования;

– этап анализа результатов моделирования.

На этапе моделирования проекты системы защиты вносятся в модель, проводится моделирование и определяется оптимальный проект. При этом решаются следующие задачи:

– создание игры против множества злоумышленников. Ввод в модель проектов системы защиты, задание их стоимости и ограничений Парето на стоимость и максимальный риск;

– создание шаблонов типов злоумышленников опасных для данной информационной системы, на основании вспомогательной таблицы;

– задание типов злоумышленников, существующих при том, или ином проекте системы защиты, и создание соответствующих игр против злоумышленника в проектах. При необходимости корректировка значений вероятности проявления определенного типа злоумышленника в конкретно взятом проекте;

– создание шаблонов угроз, существующих для информационной системы на основании списка опасных угроз;

– определение угроз, которые могут быть осуществлены, при том или ином реализованном проекте системы защиты. Угрозы включаются в игры против злоумышленников. При необходимости корректировка некоторых па-

раметров угроз, если, ущерб от осуществления угрозы или вероятность, попытки осуществления при данном проекте системы защиты отличаются от шаблонных;

– задание моделей реализации угроз (графы реализации угроз). Настройка данных моделей в соответствии с заранее собранной информацией об уязвимостях и способах их эксплуатации;

– генерация деревьев атак с использованием возможностей программного комплекса;

– проверка модели на корректность с использованием встроенных в программный комплекс механизмов;

– проведение моделирования и определение оптимального проекта системы защиты в соответствии с определенными владельцем информационной системы требованиями;

– проведение моделирования реализации дополнительных угроз и определение рисков, связанных с ними.

Разработана методика подготовки входных данных для комплекса моделей:

– модели ресурсов и угроз;

– списка наиболее опасных угроз;

– списка типов злоумышленников опасных для данной ИС;

– списка проектов СЗИ;

– списка уязвимостей СЗИ;

– графа реализации угрозы СЗИ;

– различных числовых входных данных (значений вероятностей событий, параметров законов плотности вероятности и т.д.).

В рамках разработки методики формирования списка проектов СЗИ, разработан алгоритм создания проекта СЗИ.

**В четвертой главе** выполнено моделирование системы защиты информации на примере технического университета.

Для проведения экспериментальных исследований были сформированы:

– рабочая группа, состоящая из сотрудников университета и отвечающая за сбор предварительной информации, создание проектов защиты, проведение модельных экспериментов и анализ результатов;

– экспертная комиссия, участвующая в определении входных данных для комплекса моделей.

В состав рабочей группы входили: администраторы подсетей, входящих в состав ИС; сотрудники управления по информатизации и телекоммуникациям; сотрудники деканатов и кафедр; сотрудники планово-финансового от-

дела; сотрудники отдела кадров; инженеры лабораторий университета; лаборанты. В состав экспертной комиссии входили как сотрудники университета, так и сторонние эксперты в области информационной безопасности и вычислительным сетям.

Анализ инцидентов информационной безопасности за последние несколько лет показал, что угрозы исходят, прежде всего, от студентов и сотрудников университета, а также хакеров. Причем, наибольшее количество инцидентов обусловлено действиями студентов. Инциденты, связанные с конкурентной разведкой, не фиксировались, однако это может быть обусловлено высоким уровнем подготовки злоумышленников и подробно проработанными планами атаки. Т.е. даже при осуществлении угрозы может не быть данных о проведенной атаке. Следовательно, при анализе проектов защиты нельзя игнорировать данные типы злоумышленников.

Вероятности столкновения СЗИ со злоумышленником определенного типа и вероятности попытки реализации той или иной угрозы злоумышленником определялись экспертной комиссией на основе данных полученных от рабочей группы. Для опроса использовался метод прямой оценки вероятности, а для агрегирования данных полученных от экспертов метод взвешенной суммы.

## ЗАКЛЮЧЕНИЕ

**Основные научные результаты диссертации**

1. Разработана модель реализации угрозы в информационной системе в виде полумарковского процесса, учитывающая наличие уязвимостей в СЗИ и взаимосвязей между ними.

2. Разработана игровая модель выбора оптимального проекта СЗИ по времени и вероятности реализации угрозы, стоимости проекта и величине, обобщенного риска.

3. Разработаны алгоритмы моделирования процессов реализации угрозы и поиска оптимального проекта СЗИ.

4. Разработана методика проведения моделирования системы защиты информации.

**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».

## СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

*Статьи в рецензируемых журналах*

1. Алексеев, В.Ф. Анализ методов защиты программного кода от обратного проектирования / В.Ф. Алексеев, А.В. Корвель // East European Scientific Journal. – 2019. – Т.1, № 14. – С. 19–27.

2. Алексеев, В.Ф. Постановка задачи комплексной защиты от несанкционированного доступа / В.Ф. Алексеев, А.В. Корвель // East European Scientific Journal. – 2019. – Т.1, № 14. – С. 28–35.

3. Корвель, А.В. Модель угроз обратного проектирования исполняемого кода / А.В. Корвель, В.Ф. Алексеев, Г.А. Пискун // Ежемесячный научный журнал «Евразийского Союза Ученых». – 2019. – № 5(62), Ч.2. – С. 9–15.

4. Корвель, А.В. Виртуализация программного кода псевдослучайным набором инструкций / А.В. Корвель, В.Ф. Алексеев, Г.А. Пискун // Ежемесячный научный журнал «Евразийского Союза Ученых». – 2019. – № 5(62), Ч.2. – С. 16−21.

5. Алексеев, В.Ф. Использование сетей Петри для обфускации двоичного кода алгоритма / В.Ф. Алексеев, А.В. Корвель // Scientific discussion. – 2019. – № 3(56), Ч.2. – С. 17−22.

6. Алексеев, В.Ф. Защита интрепретатора многоуровневой виртуальной машины при помощи сети Петри с возможность встраивания в стандартный процесс компиляции / В.Ф. Алексеев, А.В. Корвель // Scientific discussion. – 2019. – № 3(56), Ч.2. – С. 23−26.

*Тезисы конференций*

7. Корвель, А.В. Определение требований к системе защиты информации / А.В. Корвель // Компьютерное проектирование и технология производства электронных систем: сборник тезисов 55 научной конференции аспирантов, магистрантов и студентов, Минск, 22–26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; отв. ред. Раднёнок А. Л. – Минск, 2019. – С. 16-17.

8. Корвель, А.В. Архитектура программного комплекса и оценка адекватности модели реализации угрозы / А.В. Корвель // Компьютерное проектирование и технология производства электронных систем: сборник тезисов 54 научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. / Белорусский государственный университет информатики и радиоэлектроники; отв. ред. Раднёнок А. Л. – Минск, 2018. – С. 103-104.

## РЭЗЮМЭ

**Корвель Андрэй Віктаравіч**

**Метады і алгарытмы выбару аптымальнай сістэмы абароны інфармацыі ў інфармацыйнай сістэме арганізацыі**

***Ключавыя словы***: абарона інфармацыі, аптымальная сістэма, мадэлі рэсурсаў, мадэляванне, методыка мадэлявання.

***Мэта працы:*** распрацоўка мадэлі і метадаў для праектавання і кіравання працай сі-стемы бяспекі аб'екта, а таксама методыкі аналізу параметраў забяспечым-ня бяспекі ў гэтай сістэме.

***Атрыманыя вынікі і іх навізна:*** распрацаваны метад аналізу якасці забеспячэння бяспекі ў сістэме, якая праетуецца, што дазваляе разлічыць даступнасць і недаступнасць ўсіх аб'ектаў з улікам магчымых каналаў уцечкі, распрацавана методыка правядзення мадэліравання і выбару гарантаванасці забеспячэння палітыкі бяспекі, якая базіруецца на аналізе ацэнкі якасці падтрымання бяспекі ў інфармацыйнай сістэме. Атрыманыя вынікі дазваляюць аўтаматызаваць праектаванне структуры сістэмы бяспекі і ацаніць параметры бяспекі.

***Ступень выкарыстання:*** вынікі інтэгрыраваны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм установы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыеэлектронікі».

***Вобласць ужывання:*** абарона інфармацыі, інфармацыйныя сістэмы.

**РЕЗЮМЕ**

**Корвель Андрей Викторович**

**Методы и алгоритмы выбора оптимальной системы защиты информации в информационной системе организации**

***Ключевые слова*:** защита информации, оптимальная система, модели ресурсов, моделирование, методика моделирования.

***Цель работы*:** разработка модели и методов для проектирования и управления работой системы безопасности объекта, а также методики анализа параметров обеспечения безопасности в этой системе.

***Полученные результаты и их новизна*:** разработан метод анализа качества обеспечения безопасности в проектируемой системе, который позволяет рассчитать доступность и недоступность всех объектов с учетом возможных каналов утечки, разработана методика проведения моделирования и выбора гарантированности обеспечения политики безопасности, базирующаяся на

анализе оценки качества поддержания безопасности в информационной системе. Полученные результаты позволяют автоматизировать проектирование структуры системы безопасности и оценить параметры безопасности.

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

***Область применения*:** защита информации, информационные системы.


## SUMMARY

**Korvel Andrei Viktorovich**

**Methods and algorithms for selecting the optimal information security system in an organization's information system**

***Keywords*:** information security, optimal system, resource models, modeling, modeling methodology.

***The object of study*:** development of a model and methods for designing and controlling the operation of the object's security system, as well as methods for analyzing the parameters of ensuring security in this system.

***The results and novelty*:** developed a method for analyzing the quality of security in the projected system, which allows you to calculate the availability and inaccessibility of all objects taking into account possible channels of leakage; the system. The results obtained allow us to automate the design of the security system structure and evaluate the security parameters.

***Degree of use*:** results were integrated into the educational process at the department of design of information and computer systems of the educational institution «Belarusian State University of Informatics and Radioelectronics».

***Sphere of application***: information security, information systems.