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

УДК 004.056

*На правах рукописи*

**САВИЦКАЯ**
**Дарья Георгиевна**

# МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ОТ АТАК НА СРЕДСТВА ВИРТУАЛИЗАЦИИ

**АВТОРЕФЕРАТ**
диссертации на соискание степени
магистра технических наук

по специальности 1-38 80 04 – Технология приборостроения

Минск 2019

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

Научный руководитель: **ШНЕЙДЕРОВ Евгений Николаевич,**
кандидат технических наук, декан факультета инновационного непрерывного образования учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»,

Рецензент: **МАЗАНИК Александр Васильевич,**
кандидат физико-математических наук, доцент, заведующий кафедрой энергофизики учреждения образования «Белорусский государственный университет»

Защита диссертации состоится «26» июня 2019 г. 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

В настоящее время облачные технологии внедряются во многие сферы человеческой деятельности, в том числе активно применяются в обеспечении образовательного процесса в высших учебных заведениях. Облачные архитектуры имеют множество особенных свойств, которые делают их ценными. Базовым элементом, определяющим ключевые атрибуты облачных технологий, является виртуализация.

Технология виртуализации представляет собой инструмент для консолидации и упрощения администрирования аппаратных и программных средств. Виртуализация предоставляет множество преимуществ, помогает полноценной работе с новыми, постоянно усовершенствуемыми технологиями, беспрерывным увеличением количества информации. Поэтому внедрение облачных технологий и виртуализации в образовательный процесс открывает новый перспективный путь модернизации и повышения эффективности образования.

Несмотря на преимущества, которые предоставляют облачные технологии и виртуализация, их внедрение открывает новые угрозы и проблемы безопасности. Обеспечение безопасности виртуальной инфраструктуры является критически важным пунктом в процессе предоставления ресурсов студентам и сотрудникам, так как безопасность облачной инфраструктуры не может быть гарантирована, пока не защищена среда виртуализации. Злоумышленники могут скомпрометировать виртуальную инфраструктуру, получив доступ к физическим серверам, виртуальным машинам и информации, хранящейся на них.

Уязвимости, угрозы и основные типы атак напрямую зависят от внедренной в работу виртуальной платформы. Внедрение отдельного решения для защиты виртуальной платформы не может полностью обезопасить инфраструктуру от большого количества различных типов угроз. Анализируя основные требования и базовые принципы обеспечения безопасности, существующие современные решения в области защиты физических устройств и информации, а также учитывая основные уязвимости виртуальной платформы, разрабатывается комплекс мер по обеспечению безопасности виртуальной инфраструктуры высшего учебного заведения.

На сегодняшний день известными учеными, занимающимися проблемами безопасности облачных вычислений являются В.С. Заборовский, В.А. Курбатов, Ф. Мартинелли, С. Вогл. В их работах уделяется внимание разработке методов противодействия угрозам и созданию средств защиты информации виртуальной инфраструктуры. Разработка технологий и методов противодействия попыткам злоумышленников в получении доступа к информационным ресурсам облачных вычислений доказывает актуальность данной темы.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования**

В настоящее время облачные вычисления нашли свое применение во многих областях человеческой деятельности и продолжают активно развиваться. Внедрение облачных технологий в образовательный процесс позволяет повысить качество подготовки и переподготовки специалистов, кроме того позволяет улучшить наглядность занятий, при этом происходит экономия аппаратных ресурсов и затрат на обслуживание компьютерных классов. Зачастую, обеспечение безопасности облачного сервиса ограничивается защитой физической инфраструктуры и информации, не учитывая особенности технологии облачных вычислений. Облачные технологии строятся на базе виртуализации, которая открывает большое количество различных типов угроз облачной инфраструктуры.

В связи с вышесказанным, актуальной является поиск и разработка методов и средств обеспечения безопасности средств виртуализации.

**Степень разработанности проблемы**

Исследование методов и средств обеспечения безопасности виртуализации осуществлялось на основе анализа существующей системы, с использованием методик и работ зарубежных авторов.

Одной из слабых сторон исследований в современных работах является недостаточно полное рассмотрение возможных угроз средств виртуализации.

Предложенное исследование направлено на устранение данного недостатка, основывается на проведении исследования современных методов и средств обеспечения безопасности определенной платформы виртуализации, а также определению конкретных угроз для выбранной платформы.

**Цель и задачи исследования**

*Целью* данной работы является поиск возможных угроз облачных вычислений, а также разработка защищенной виртуальной инфраструктуры учреждения высшего образования.

Для достижения поставленной цели в ходе работы необходимо решить следующие *задачи*:

1. Провести анализ существующей облачной инфраструктуры учреждения высшего образования.
2. Изучить существующие угрозы безопасности, рассматриваемой информационной системы учреждения высшего образования.
3. Разработать комплекс мер для обеспечения безопасной инфраструктуры, а также выполнить их реализацию.

*Объектом* исследования является виртуализация высшего учебного заведения.

*Предметом* исследования является поиск и изучение методов и средств защиты информации в частном облачном сервисе учреждения высшего образования.

**Область исследования**

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

**Теоретическая и методологическая основа исследования**

В основу диссертации легли работы зарубежных ученых в области защиты виртуальной инфраструктуры.

*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 определении методов, средств и научных подходов обеспечения защищенной облачной инфраструктуры для студентов и сотрудников учреждения высшего образования.

*Теоретическая значимость* работы заключается в детальном анализе существующей облачной инфраструктуры учреждения высшего образования, а также в исследовании найденных уязвимостей, угроз и основных типов атак в виртуальной инфраструктуре.

*Практическая значимость* диссертации состоит в определении комплекса методов и средств, применяемых для обеспечения безопасности инфраструктуры.

**Основные положения, выносимые на защиту**

1. Систематизация работы частной облачной инфраструктуры высшего учебного заведения, основанная на анализе доступной технической документации.

2. Определение и классификация угроз, уязвимостей и основных типов атак, которые позволяют сделать вывод о необходимых методах и средствах защиты виртуальной инфраструктуры высшего учебного заведения.

3. Рекомендации для построения защищенного частного облака учреждения высшего образования.

**Апробация диссертации и информация об использовании ее результатов**

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 55-ой научной конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Беларусь, 2019 г).

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в лекционный курс «Основы компьютерной техники и программирования мобильных электронных систем».

**Публикации**

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах. В их числе 1 статья в сборнике материалов научной конференции и 3 статьи в научных рецензируемых журналах.

**Структура и объем работы**

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

**В первой главе** приведен обзор принципов организации облачных вычислений, а также технологий виртуализации. Выполнен детальный анализ платформы виртуализации, а также архитектуры частного облака высшего учебного заведения.

**Во второй главе** представлен анализ угроз безопасности, направленных на информационную систему. Выделены особенности угроз и уязвимостей виртуализации.

**В третьей главе** представлен комплекс методов и средств по защите рассматриваемой инфраструктуры от угроз безопасности. Также выполнено внедрение данного комплекса в виртуальную инфраструктуру частного облака высшего учебного заведения.

**В приложении** представлены схема структуры частного облака высшего учебного заведения, функциональная схема частного облака высшего учебного заведения, схема адресации виртуальной сетевой инфраструктуры, публикации автора, акт внедрения и отчет о проверке на антиплагиат.

Общий объем диссертационной работы составляет 102 страницы. Из них 65 страниц основного текста, 6 иллюстраций, 1 таблица, библиографический список из 56 наименований на 5 страницах, список собственных публикаций соискателя из 4 наименований, 7 приложений на 30 страницах.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы безопасности облачных вычислений для высшего учебного заведения, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

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** рассмотрены принципы организации облачных вычислений, их основные характеристики, различные типы облаков – частное, публичное, гибридное – и связанные с ними преимущества и недостатки.

Дана краткая характеристика моделей обслуживания в облачных вычислениях: инфраструктура как услуга, когда пользователь получает в распоряжение набор виртуальных ресурсов (виртуальных машин), платформа как услуга, когда пользователь получает какой-то сервис (базу данных, службу обмена сообщениями и т. д.) для использования в своём приложении, и программное обеспечение, когда через тонкий клиент пользователь получает готовое приложение.

На основании полученной характеристики сделан вывод о том, что самым оптимальным вариантом для учреждения высшего образования, исходя из найденных недостатков и преимуществ, является гибридное облако. Для работы студентов и сотрудников оптимально предоставлять такие сервисы, как «Программное обеспечение как услуга» и «Инфраструктура как услуга».

Также представлена взаимосвязь основных терминов, принятых в виртуализации и их краткая характеристика. Приведены преимущества и недостатки, которые дает внедрение технологии виртуализации в центр обработки данных организации.

На основании полученной информации сделан вывод, что внедрение виртуализации в образовательный процесс открывает перспективный путь развития и повышения эффективности подготовки и переподготовки специа-

листов.

Глубоко изучена платформа VMware vSphere, на базе которой построено частное облако учреждения образования «Белорусский государственный университет информатики и радиоэлектроники». Рассмотрены основные компоненты платформы (рисунок 1).

При проведении исследования выявлено, что данная платформа имеет закрытый исходный код, а самыми уязвимыми являются следующие компоненты:

- виртуальная машина;
- гипервизор;
- сервер управления;
- система хранения данных;
- виртуальная сеть.

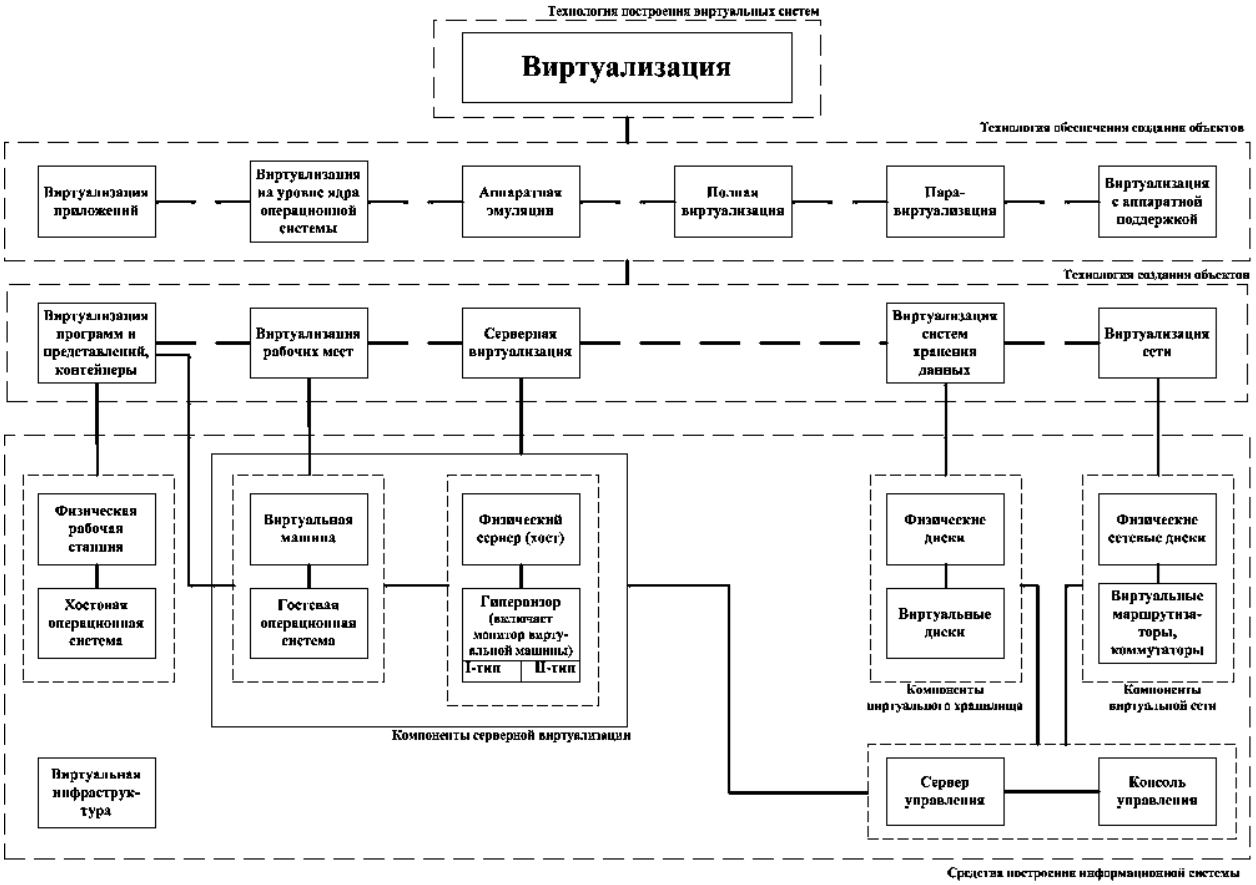


Рисунок 1 – Основные компоненты платформы виртуализации

Подробно изучена архитектура частного виртуального облака учреждения образования «Белорусский государственный университет информатики и радиоэлектроники». В соответствии с текущей конфигурацией была представлена и описана структурная схема частного облака университета, схема подключения физических устройств, а также схема адресации исследуемой

инфраструктуры, рассмотрена установка оборудования в серверной комнате.

В процессе анализа архитектуры частного облака были выявлены основные компоненты (рисунок 2), которые требуют защиты от угроз безопасности:

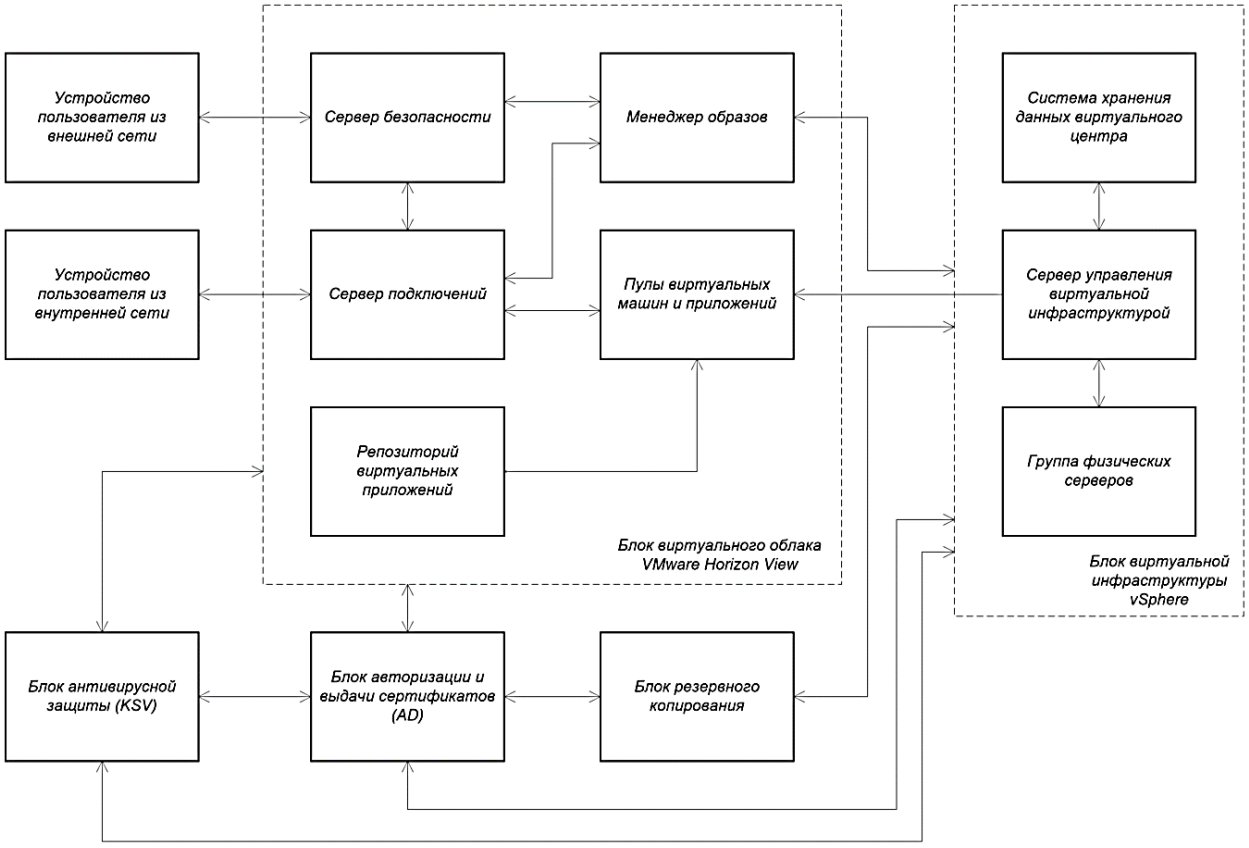


Рисунок 2 – Основные компоненты частного облака
высшего учебного заведения

- аппаратная часть;
- хранилище;
- виртуальная сеть;
- кластер ESXi-серверов;
- сервер синхронизации учетных данных для Microsoft Office 365;
- серверы Active Directory;
- vCenter Server;
- View Composer;
- Connection Server;
- Security Server;
- терминальные сервера;
- виртуальные рабочие столы;
- виртуальные приложения пользователей;
- сервер антивирусной защиты для виртуальных сред.

**Во второй главе** рассмотрены основные понятия в области угроз безопасности, рассмотрены типы современных злоумышленников, их основные характеристики, а также представлена классификация угроз безопасности по ряду критериев. Подробно изучены угрозы физической и информационной инфраструктуры.

Сделан вывод, что информационная система защищена на столько, на сколько защищен самый слабый компонент инфраструктуры. Одним из самых опасных источников угроз являются внутренние угрозы, то есть угрозы со стороны сотрудников организации. К распространенным угрозам со стороны вредоносного программного обеспечения относят: вирусы, черви, троянские кони, логические бомбы, вымогатели, бэкдоры и руткиты.

К атакам по электронной почте и через браузер относят: спам, рекламное программное обеспечение, программы-шпионы, фишинг, вишинг, смишинг, фарминг, угонщик браузера.

Самыми опасными среди всех атак являются атаки социальной инженерии и методы обмана.

Досконально изучены угрозы, недостатки и уязвимости, которые отличают виртуальную инфраструктуру от традиционной. Выделены основные угрозы виртуализации, такие как:

- раскрытие;
- обман;
- сбой;
- незаконный захват.

Дана их краткая характеристика. Изучен общий классификатор уязвимостей и недостатков программного обеспечения. Рассмотрены основные слабые стороны виртуализации, среди которых: внедрение, неверная аутентификация, управление учетными записями, управление разрешениями и привилегиями, криптографические проблемы, обработка данных, ошибки управления информацией, неполная проверка ввода, недостаточная проверка подлинности данных, недостаточная проверка сертификата, использование недостаточно случайных значений, ошибки управления ресурсами, состояние гонки, среда, конфигурация.

Также рассмотрены уязвимости виртуальной инфраструктуры с учетом возможных последствий для операционных систем, гипервизора, сети и хранилища.

В ходе проведенного исследования сделан вывод о том, что крайне необходимо защищать аппаратную и программную часть инфраструктуры, а также информацию, учитывая особенности облачных вычислений. Это связано с тем, что внедрение виртуализации усугубляет действие распространенных угроз безопасности, а также привносит большое количество новых угроз.

**В третьей главе** рассмотрены основные понятия в данной области, рассмотрен куб кибербезопасности, подробно изучены грани данного куба. Дана полная характеристика состояния данных, принципов безопасности, а также контрмер. Кроме того, рассмотрена модель кибербезопасности, которая показывает задачи безопасности и понимание подходов к их решению.

На основании полученных результатов сделан вывод, что информация, находясь в одном из трех состояний: (хранение, передача, обработка) должна соответствовать всем трем принципам безопасности (конфиденциальность, целостность, доступность), что достигается при помощи технологий, внедрения политик и практик, а также влияния человеческого фактора. Кроме того, для обеспечения безопасности можно использовать модель кибербезопасности, состоящую из двенадцати независимых доменов для понимания сложных задач безопасности и подходов к их решению.

На основании базовых принципов обеспечения безопасности определены меры и средства защиты физических устройств, информации, а также виртуальной инфраструктуры от атак. Определен ряд мер обеспечения безопасности платформы виртуализации VMware для таких компонентов, как гипервизор, виртуальная машина, виртуальная сеть, системы хранения, сервер управления.

В результате проделанного исследования внедрение методов и средств обеспечения безопасности облачных вычислений от атак на средства виртуализации была получена защищенная отказоустойчивая инфраструктура, поддерживающая целостность и конфиденциальность данных.

## ЗАКЛЮЧЕНИЕ

**Основные научные результаты диссертации**

1. Выявлено, что самым оптимальным вариантом для учреждения высшего образования, исходя из найденных недостатков и преимуществ, является сочетание частного и публичного облаков. Выполнение глубокого анализа частной облачной инфраструктуры высшего учебного заведения, показало, что внедрение виртуализации привносит в информационную систему организации большой ряд новых компонентов, которые требуют защиты от угроз безопасности [1].

2. Определены и исследованы наиболее распространенные угрозы и уязвимости безопасности, которым подвергаются информационные системы, основанные на виртуализации. В ходе исследования было выявлено, что одним из самых опасных источников угроз являются внутренние угрозы, то есть угрозы со стороны сотрудников организации.

Кроме того, внедрение виртуализации усугубляет действие распространенных угроз безопасности, а также привносит большое количество новых угроз [2, 4].

3. Исходя из особенностей рассмотренной облачной инфраструктуры и обозначенных угроз и уязвимостей определен комплекс мер по обеспечению безопасности облачной инфраструктуры учреждения высшего образования, полученные результаты показывают, что внедрение отдельного решения не сможет полностью обезопасить инфраструктуру от большого количества различных типов угроз, поэтому средства и методы по обеспечению безопасности следует внедрять комплексно на нескольких уровнях. Данный комплекс позволяет обеспечивать непрерывную защиту информационной системы [3].

**Рекомендации по практическому использованию результатов**

На основании результатов исследований возможно построение информационных систем на основе виртуализации, которые будут удовлетворять современным стандартам безопасности.

Полученные результаты внедрены в учебный процесс на кафедре проектирвоания информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в лекционный курс «Основы компьютерной техники и программирования мобильных электронных систем».

## СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

*Статьи в рецензируемых журналах*

1. Игнатович Р.О., Савицкая Д.Г., Мигалевич С.А., Марков А.Н. Внедрение облачных решений в образовательный процесс / Игнатович Р.О., Савицкая Д.Г., Мигалевич С.А., Марков А.Н. // Центр молодежных инноваций минский городской технопарк – Минск: 2018, с.67.

2. Савицкая Д.Г., Мигалевич С.А., Основные угрозы безопасности виртуализации / Савицкая Д.Г., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка» (в печати).

3. Савицкая Д.Г., Мигалевич С.А. Защита центра обработки данных от угроз безопасности / Савицкая Д.Г., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка» (в печати)

4. Калиновская А.А., Савицкая Д.Г. Анализ существующих методов и средств обеспечения безопасности информации и виртуализации в высшем учебном заведении / Калиновская А.А., Савицкая Д.Г. // Материалы работы 55-й научной конференции аспирантов, магистрантов и студентов БГУИР. – Минск: БГУИР апрель 2019 (в печати).

# РЭЗЮМЭ

**Савіцкая Дар'я Георгіеўна**

**Метады і сродкі для абароны воблачных вылічэнняў ад нападаў на сродкі віртуалізацыі**

***Ключавыя словы***: бяспека, воблачныя вылічэнні, віртуалізацыя.

***Мэта працы:*** даследаванне пагроз воблачных вылічэнняў, а таксама распрацоўка абароненай віртуальнай інфраструктуры ўстановы вышэйшай адукацыі.

***Атрыманыя вынікі і іх навізна:*** у ходзе даследавання выяўлена, што самым аптымальным варыянтам для ўстановы вышэйшай адукацыі, зыходзячы з знойдзеных недахопаў і пераваг, з'яўляецца спалучэнне прыватнага і публічнага аблокаў. Выкананне глыбокага аналізу прыватнай воблачнай інфраструктуры вышэйшай навучальнай установы, паказала, што ўкараненне віртуалізацыі прыўносіць ў інфармацыйную сістэму арганізацыі вялікі шэраг новых кампанентаў, якія патрабуюць абароны ад пагроз бяспекі

Вызначаны і даследаваны найбольш распаўсюджаныя пагрозы і ўразлівасці бяспекі, якім падвяргаюцца інфармацыйныя сістэмы, заснаваныя на віртуалізацыі. У ходзе даследавання было выяўлена, што адным з самых небяспечных крыніц пагроз з'яўляюцца ўнутраныя пагрозы, то ёсць пагрозы з боку супрацоўнікаў арганізацыі. Акрамя таго, ўкараненне віртуалізацыі пагаршае дзеянне распаўсюджаных пагроз бяспекі, а таксама прыўносіць вялікая колькасць новых пагроз.

Зыходзячы з асаблівасцяў разгледжанай воблачнай інфраструктуры і пазначаных пагроз і ўразлівасцяў вызначаны комплекс мер па забеспячэнні бяспекі воблачнай інфраструктуры ўстановы вышэйшай адукацыі, атрыманыя вынікі паказваюць, што ўкараненне асобнага рашэння не зможа цалкам засцерагчы інфраструктуру ад вялікай колькасці розных тыпаў пагроз, таму сродкі і метады па забеспячэнні бяспекі варта ўкараняць комплексна на некалькіх узроўнях. Дадзены комплекс дазваляе забяспечваць бесперапынную абарону інфармацыйнай сістэмы.

***Ступень выкарыстання:*** На падставе вынікаў даследаванняў магчыма пабудова інфармацыйных сістэм на аснове віртуалізацыі, якія будуць задавальняць сучасным стандартам бяспекі.

Атрыманыя вынікі ўкаранёны ў вучэбны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» у лекцыйны курс «Асновы камп'ютарнай тэхнікі і праграмавання мабільных электронных сістэм».

***Вобласць ужывання:*** установы вышэйшай адукацыі.

# РЕЗЮМЕ

## Савицкая Дарья Георгиевна

## Методы и средства защиты облачных вычислений от атак на средства виртуализации

**Ключевые слова:** безопасность, облачные вычисления, виртуализация.

**Цель работы:** исследование угроз облачных вычислений, а также разработка защищенной виртуальной инфраструктуры учреждения высшего образования.

**Полученные результаты и их новизна:** в ходе исследования выявлено, что самым оптимальным вариантом для учреждения высшего образования, исходя из найденных недостатков и преимуществ, является сочетание частного и публичного облаков. Выполнение глубокого анализа частной облачной инфраструктуры высшего учебного заведения, показало, что внедрение виртуализации привносит в информационную систему организации большой ряд новых компонентов, которые требуют защиты от угроз безопасности.

Определены и исследованы наиболее распространенные угрозы и уязвимости безопасности, которым подвергаются информационные системы, основанные на виртуализации. В ходе исследования было выявлено, что одним из самых опасных источников угроз являются внутренние угрозы, то есть угрозы со стороны сотрудников организации. Кроме того, внедрение виртуализации усугубляет действие распространенных угроз безопасности, а также привносит большое количество новых угроз.

Исходя из особенностей рассмотренной облачной инфраструктуры и обозначенных угроз и уязвимостей определен комплекс мер по обеспечению безопасности облачной инфраструктуры учреждения высшего образования, полученные результаты показывают, что внедрение отдельного решения не сможет полностью обезопасить инфраструктуру от большого количества различных типов угроз, поэтому средства и методы по обеспечению безопасности следует внедрять комплексно на нескольких уровнях. Данный комплекс позволяет обеспечивать непрерывную защиту информационной системы.

**Степень использования:** на основании результатов исследований возможно построение информационных систем на основе виртуализации, которые будут удовлетворять современным стандартам безопасности.

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радио-электроники» в лекционный курс «Основы компьютерной техники и программирования мобильных электронных систем».

**Область применения:** учреждения высшего образования.

**SUMMARY**

**Savitskaya Darya Georgievna**

**Methods and tools to protect cloud computing from attacks on virtualization**

***Keywords*:** security, cloud computing, virtualization.

***The object of study*:** studying the threats of cloud computing, as well as the construction of a secure virtual infrastructure of a higher education institution.

***The results and novelty*:** the study revealed that the best option for the establishment of higher education, based on the found disadvantages and advantages, is a combination of private and public clouds. An in-depth analysis of the private cloud infrastructure of a higher education institution has shown that the introduction of virtualization brings a large number of new components to the organization's information system that require protection against security threats.

Identified and investigated the most common threats and security vulnerabilities, which are exposed to information systems based on virtualization. The study revealed that one of the most dangerous sources of threats are internal threats, that is, threats from employees of the organization. In addition, the introduction of virtualization exacerbates the effect of common security threats, and also introduces a large number of new threats.

Based on the characteristics of the considered cloud infrastructure and the identified threats and vulnerabilities, a set of measures to ensure the safety of the cloud infrastructure of a higher education institution is determined, the results show that the implementation of a separate solution will not fully protect the infrastructure from a large number of different types of threats, therefore the means and methods to ensure security should be implemented comprehensively at several levels. This complex allows you to provide continuous protection of the information system.

***Degree of use*:** based on the research results, it is possible to build information systems based on virtualization, which will meet modern security standards.

The obtained results were implemented into the educational process at the department of design of information-computer systems of the educational institution "Belarusian State University of Informatics and Radioelectronics" in the lecture course "Fundamentals of computer technology and programming of mobile electronic systems".

***Sphere of application***: institutions of higher education.