Бурса Максим Васильевич. Отказ в обслуживании мультисервисных сетей по протоколу HTTP: анализ и регулирование рисков: диссертация ... кандидата технических наук: 05.13.19 / Бурса Максим Васильевич;[Место защиты: Воронежский государственный технический университет].- Воронеж, 2015.- 142 с.

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный технический университет»

На правах рукописи



БУРСА Максим Васильевич

**ОТКАЗ В ОБСЛУЖИВАНИИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ ПО ПРОТОКОЛУ HTTP: АНАЛИЗ И РЕГУЛИРОВАНИЕ РИСКОВ**

05.13.19 Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель

доктор технических наук, профессор

Остапенко Григорий Александрович

Воронеж - 2015

**Оглавление**

ВВЕДЕНИЕ 4

1. МУЛЬТИСЕРВИСНЫЕ СЕТИ КАК ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ DDOS-ATAK 13
   1. Мультисервисные сети. Типы и особенности построения 13
      1. [Типы мультисервисных сетей 14](#bookmark1)
      2. Особенности мультисервисных сетей 19
   2. Распределенные атаки типа «отказ в обслуживании» как угроза безопасности мультисервисных сетей ; 21
      1. [Основные механизмы реализации DDoS-атак 22](#bookmark2)
      2. [Основные типы DDoS-атак 30](#bookmark4)
      3. Классификация механизмов защиты от DDoS-атак 40
   3. Необходимость развития методологии риск-анализа для мультисервисных сетей как объекта защиты информации 42
   4. [Выводы по первой главе 44](#bookmark5)
2. АНАЛИТИЧЕСКАЯ ОЦЕНКА УЩЕРБА И РИСКА РЕАЛИЗАЦИИ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» ПО ПРОТОКОЛУ HTTP НА МУЛЬТИСЕРВИСНЫЕ СЕТИ 45
   1. Определение аналитического вида функции ущерба реализации атак типа «отказ в обслуживании» по протоколу HTTP на компоненты мультисервисных сетей 45
   2. Обоснование выбора и доказательство гипотезы относительно плотности вероятности наступления ущерба при реализации атак типа «отказ в обслуживании» по протоколу HTTP на компоненты мультисервисных сетей 47
   3. Определение шага дискретизации переменной функции риска при реализации атак типа «отказ в обслуживании» по протоколу HTTP на компоненты мультисервисных сетей 53
   4. Оценка параметров риска компонента мультисервисной сети при реализации на него атаки типа «отказ в обслуживании» по протоколу HTTP 57
   5. Оценка параметров риска компонент мультисервисных сетей при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP с использованием огибающей функции риска 65
   6. Дискретная оценка риска компонент мультисервисных сетей при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP 69
   7. Численное моделирование риска мультисервисной сети, включающей

несколько web-серверов 72

[2.7. Выводы по второй главе 75](#bookmark35)

3 УПРАВЛЕНИЕ РИСКАМИ И ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ МУЛЬТИСЕРВИСНЫХ СИСТЕМ, ПОДВЕРГАЮЩИХСЯ АТАКАМ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» ПО ПРОТОКОЛУ HTTP 76

1. Исследование динамических свойств функции риска к изменению ее параметров 76
2. Управление риском компонент мультисервисной сети при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP 96
3. Алгоритм управления риском мультисервисных сетей подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP 114
4. Оценка эффективности защиты мультисервисных сетей при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP 120
5. [Выводы по третьей главе 123](#bookmark45)

ЗАКЛЮЧЕНИЕ 124

126

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ПРИЛОЖЕНИЕ А

**ВВЕДЕНИЕ**

Актуальность темы исследования. Анализ и управление информационными рисками в системах различного характера и масштаба в настоящее время становится одной из ключевых задач в деятельности не только структурных подразделений и организаций по защите информации, но и государства в целом. В то же время профессия хакера становится все более выгодной, так как реализация атак стала средством эффективной конкурентной борьбы. Количество реализуемых угроз постоянно возрастает, что говорит о широких возможностях для злоумышленников по осуществлению различных деструктивных воздействий [61-67]. Одной из наиболее актуальных угроз являются DDoS-атаки, сила и частота реализации которых неуклонно растет, а самим атакам подвергаются сайты не только коммерческих компаний, но и государственных ресурсов [68-72]. Увеличению количества атак способствует развитие сетевых структур, а также различных способов и средств информационного взаимодействия в информационно-телекоммуникационных системах, широкое распространение среди которых получили мультисервисные сети (МСС), в силу того, что они интегрируют различные виды сервисов воедино, среди которых: передача речи, видеотелефония, доступ к базам данных, доступ к ресурсам файл-серверов, доступ в Интернет, электронная почта, доступ к ресурсам web-серверов [13, 27]. Данные сети способны передавать разнородную информацию с высокой скоростью, что упрощает процедуру взаимодействия между пользователями, а также процесс управления МСС [26, 74]. Но, так как в составе подобных сетей зачастую функционирует **web-cepBep,** они подвержены атакам типа «отказ в обслуживании» по протоколу HTTP, по причине простоты их реализации и недостатка внимания к данной угрозе при проектировании сетей [85]. Атаки данного типа производятся в отношении web-серверов МСС с использованием протокола HTTP. Актуальность исследования обусловлена следующими противоречиями:

* ростом силы, частоты и продолжительности атак типа «отказ в обслуживании» по протоколу HTTP и низким уровнем защищенности МСС от данного вида деструктивного воздействия;
* между потребностью субъектов обеспечения безопасности атакуемых посредством атак типа «отказ в обслуживании» по протоколу HTTP МСС в научно обоснованных методах их риск-анализа и готовностью науки предоставить таковые для эффективного использования;
* между значимостью обоснованного применения средств защиты информации web-серверов, входящих в состав МСС, и практической реализацией мер защиты информации в МСС в целях снижения информационных рисков успеха осуществления атак типа «отказ в обслуживании» по протоколу HTTP на них.

В связи с этим представляется актуальным развитие научно-методического обеспечения в данной области, включая изучение угроз, возникающих при проведении атак типа «отказ в обслуживании» по протоколу HTTP на МСС, и связанных с ними рисков с точки зрения оценки и управления этими рисками с целью повышения защищенности как компонентов МСС, так и сетей в целом.

Степень разработанности темы исследования. Касательно вопросов обеспечения информационной безопасности [1, 3-5, 6, 9, 11, 12, 24, 25, 35-38, 41, 46-48, 54, 75, 91] и, в частности, методов защиты от DDoS-атак, а также особенностей их реализации, опубликовано значительное количество работ, в которых проанализированы как сами атаки, так и возможные меры и средства для противодействия им [43, 58, 77-84, 93]. Вместе с тем, методология риск-анализа в части статических риск-моделей и исследования информационных рисков в динамике применялась к широкому кругу систем [5, 76, 88, 89, 94], таких как распределенные информационные системы [42, 44, 50-52, 55, 60, 99], информационно-телекоммуникационные системы [43, 59], социальные

информационные системы [49, 90, 100], распределенные платежные системы [29], функционирующие в условиях реализации различных атак, среди которых: блокирующие доступ к ресурсам системы [92, 97], вирусные атаки [56, 57, 101], компьютерные атаки [34], внедрение вредоносного программного обеспечения [87]. Также рассматривались вопросы управления рисками [31-33, 39, 40, 52, 53] и оценки живучести систем [23, 99]. Однако в данной области не исследовались вопросы оценки и регулирования риска и эффективности защиты компонентов мультисервисных сетей, а также определения величины ущербов, возникающих в МСС при реализации атак типа «отказ в обслуживании» по протоколу HTTP. Таким образом, совершенствование методологии риск-анализа в целях повышения защищенности МСС от атак типа «отказ в обслуживании» по протоколу HTTP на основе оценки и регулирования рисков представляется актуальным.

Отсюда вытекает научно-техническая задача диссертации: развитие научно-методического обеспечения и выработка технических решений для оценки и регулирования рисков МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP.

Диссертационная работа выполнена в соответствии с одним из основных направлений ФГБОУ ВПО «Воронежский государственный технический университет» «Управление информационными рисками и обеспечение безопасности инфокоммуникационных технологий» на базе Воронежского научно-образовательного центра управления информационными рисками.

Объектом исследования являются МСС, в отношении которых реализуются атаки типа «отказ в обслуживании» по протоколу HTTP.

Предметом исследования является риск-анализ успешной реализации на МСС атак типа «отказ в обслуживании» по протоколу HTTP и управление их защищенностью посредством настройки средств защиты информации для web- серверов, функционирующих в их составе.

Цель исследования состоит в повышении эффективности защиты и управлении защищенностью web-серверов МСС при реализации атак типа «отказ в обслуживании» по протоколу HTTP. Для достижения цели представляется необходимым решить следующие задачи:

1. Создание риск-модели для web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP, основанной на статистике ущербов и аналитически связывающей параметры web-серверов и средств их защиты.
2. Разработка методики управления риском web-серверов, функционирующих в составе МСС и атакуемых по протоколу HTTP, посредством настройки средств защиты информации для повышения их защищенности.
3. На базе полученных риск-моделей, разработка методики определения эффективности защиты web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP.

На защиту выносятся:

1. Риск-модель web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP, основанная на статистике ущербов и аналитически связывающая параметры риска с параметрами web-серверов и средствами их защиты.
2. Методика управления риском web-серверов, функционирующих в составе МСС, реализованная на базе теории динамического риск-анализа и позволяющая посредством изменения физических характеристик web-серверов и связанного с ними оборудования регулировать значения риска атакуемых серверов в заданном временном интервале.
3. Аналитические выражения для мгновенной и интегральной оценки эффективности защиты МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP.

Научная новизна результатов:

1. Предлагаемая риск-модель web-серверов МСС отличается от аналогичных учетом физических характеристик web-серверов и связанного с ними оборудования МСС, а также атак типа «отказ в обслуживании» по протоколу HTTP.
2. Методика управления риском web-серверов, входящих в состав МСС, отличается от аналогичных разработанным алгоритмом управления, учитывающим влияние изменений внутренних характеристик МСС и ее web- серверов на изменение других параметров во времени, на коэффициенты чувствительности риска и на функцию дополнительного движения риска объекта атаки, с учетом которых предлагаются объективные методы для снижения риска атакуемого объекта.
3. В предложенных оценках уровня защищенности web-серверов МСС, при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP, впервые вводится оценка эффективности защиты МСС, базирующаяся на полученных риск-моделях.

Теоретическая значимость работы, состоит в том, что:

* доказаны положения, вносящие вклад в расширение представлений о явлении успешных реализаций атак типа «отказ в обслуживании» на web-серверы МСС по протоколу HTTP;
* применительно к проблематике диссертации, с получением обладающих новизной результатов, использован аппарат теории риск-анализа в отношении реализации атак типа «отказ в обслуживании» на web-серверы МСС по протоколу HTTP;
* изложены положения и элементы теории для аналитической оценки ущерба, риска и эффективности защиты web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP;
* раскрыты противоречия между значимостью проблемы защиты web- серверов МСС и адекватностью моделей и методик оценки и управления их защищенностью от атак типа «отказ в обслуживании», реализуемых по протоколу HTTP;
* изучены внутренние и внешние противоречия, факторы и причинно­следственные связи, порождающие информационные риски успешной реализации атак типа «отказ в обслуживании» на web-серверы МСС по протоколу HTTP;
* проведена модернизация существующих математических моделей и алгоритмов, обеспечивающая возможность аналитической оценки и управления рисками, а также оценки эффективности защиты web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP, с использованием теории чувствительности функций и учетом особенностей атак и физических характеристик серверов.

**Практическая ценность работы** заключается в том, что:

* разработаны и внедрены в учебный и производственный процесс новые универсальные методики риск-анализа и оценки защищенности атакуемых по протоколу HTTP web-серверов, функционирующих в составе МСС;
* определены перспективы практического использования предложенных методик для повышения защищенности web-серверов МСС от реализации атак типа «отказ в обслуживании» по протоколу HTTP;
* создана система практических рекомендаций для управления рисками реализации атак типа «отказ в обслуживании» на web-серверы МСС по протоколу HTTP;
* представлены предложения по дальнейшему совершенствованию, с использованием аппарата теории риск-анализа, процесса управления информационными рисками, базирующегося на теории чувствительности и учитывающего физические характеристики реализации разнообразных атак типа «отказ в обслуживании» и систем различного характера для повышения их защищенности.

**Методы исследования. В** исследовании используются методы системного анализа, теории вероятностей и математической статистики, математического анализа, теории чувствительности функций, методы теории рисков.

**Соответствие специальности научных работников.** Полученные научные результаты соответствуют следующим пунктам паспорта специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность»: анализ риска нарушения безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения (п. 7); модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты (п. 10); модели и методы управления информационной безопасностью (п. 15).

**Степень достоверности научных положений и выводов,**

сформулированных в исследовании, подтверждаются тем, что:

* теория построена на известных, проверяемых фактах статистического исследования реализации атак типа «отказ в обслуживании» на web-серверы МСС по протоколу HTTP, что согласуется с опубликованными данными в области риск-анализа;
* идея базируется на анализе практики и обобщении передового отечественного и зарубежного опыта в области оценки и управления рисками реализации атак типа «отказ в обслуживании» на системы различного характера, представленного в нормативных документах;
* использовано сравнение авторских данных с результатами, полученными ранее, по рассматриваемой области в работах член-корр. РАН Новикова Д.А. [39, 40], член-корр. РАН Борисова В.И. [52], д. техн. наук Остапенко А.Г. [42-45, 98], д. техн. наук Калашникова А.О. [30, 31, 95];
* установлено качественное совпадение авторских результатов с результатами, представленными в работах Тишкова С.А. в области риск-анализа различных систем при отказах в обслуживании [79-84], а также с результатами, полученными д. техн. наук Зегждой П.Д. [28], д. техн. наук Лосем В.П. [8], д. техн. наук Калашниковым А.О. [30, 31, 95], д. техн. наук Громовым IO.IO. [22, 23] и канд. техн. наук Симоновым К.В. [49] в области оценки эффективности защиты инфокоммуникационных систем при реализации на них деструктивных информационных воздействий;
* использованы современные методики сбора и обработки информации, включая, предоставленные ведущими отечественными и зарубежными организациями в области защиты и информации, выборочные совокупности численных значений частоты реализаций атак типа «отказ в обслуживании» по протоколу HTTP.

**Внедрение результатов работы.** Полученные основные научные результаты диссертационного исследования используются в ФГБОУ ВПО «Воронежский государственный технический университет» в учебном процессе на кафедре систем информационной безопасности при организации изучения специальных дисциплин в ходе подготовки специалистов по специальности 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем», что подтверждено актом о внедрении в учебный процесс, а также в ОАО «Банк Москвы» для управления риском при эксплуатации его МСС.

**Апробация работы.** Основные результаты исследований и научных разработок докладывались и обсуждались на Межрегиональной научно­практической конференции «Инновации и информационные риски» (Воронеж, 2012, 2013 и 2014 гг.), Всероссийской научно-технической конференции «Перспективные исследования и разработки в области информационных технологий и связи» (Воронеж, 2013 и 2014 гг.), Межвузовской неделе науки в сфере информационной безопасности (Воронеж, 2013 и 2014 гг.), Всероссийской конференции «XII всероссийское совещание по проблемам управления» (Москва -2014).

**Публикации.** По теме диссертации опубликовано 23 научные работы, в том числе 10 - в изданиях, рекомендованных ВАК РФ, а также 1 учебное пособие, 2 монографии и 1 статья в издании по перечню SCOPUS.

**Личный вклад автора.** Все основные результаты работы получены автором самостоятельно. В работах, опубликованных в соавторстве, лично автору принадлежат: подход к оценке экстремумов интегрального риска распределенных ресурсов инновационных проектов при реализации в отношении них DDoS-атак [102]; аналитические модели реализации атак типа «НТТР-флуд», построенные на базе аппарата теории сетей Петри-Маркова [103, 117]; подходы к управлению рисками информационно-телекоммуникационных систем при реализации в их отношении атак типа «отказ в обслуживании» [104, 119]; аналитическая риск- модель инновационного проекта, подвергающегося распределенным атакам типа «отказ в обслуживании» [105]; подход к оценке защищенности ресурсов информационно-телекоммуникационных систем при реализации в их отношении

DDoS-атак [106]; аналитическое обоснование функции ущерба при реализации атак типа «НТТР-флуд» [107, 121]; методы по управлению защищенностью информационно-телекоммуникационных систем, подвергающихся атакам типа «НТТР-флуд» [109]; аналитические оценки риска реализации распределенных атак типа «НТТР-флуд» на многокомпонентные информационно­телекоммуникационные системы [110]; аналитическая оценка шага дискретизации при реализации атак типа «НТТР-флуд» на компоненты информационно-телекоммуникационных систем, а также подход к оценке их возможной эффективности [111]; исследование механизмов реализации DDoS- атак, а также классификация существующих атак типа «отказ в обслуживании» и механизмов защиты от них [112]; исследование специфики реализации флуд-атак

1. ; оценка риска сложных систем на основе параметров рисков их компонентов
2. ; имитационная модель реализации атаки типа «НТТР-флуд» на сетевые структуры [118]; аналитические выражения моды и пика функции риска при реализации атак типа «НТТР-флуд» на компоненты ИТКС [120]; аналитическая оценка ущерба и риска реализации атак типа «НТТР-флуд» на мультисервисные сети [122]; дискретная риск-модель реализации атак типа «НТТР-флуд» на мультисервисные сети [123]; подход к управлению ущербом при реализации флуд-атак по гипертекстовому протоколу передачи информации [124].

Структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, списка литературы, включающего 124 наименования, одного приложения. Основная часть работы изложена на 142 страницах, содержит 43 рисунка и 10 таблиц. Приложение содержит документы, подтверждающие практическое использование и внедрение результатов диссертационного исследования.

**ЗАКЛЮЧЕНИЕ**

Работа посвящена разработке методик для оценки информационных рисков реализации атак типа «отказ в обслуживании» по протоколу HTTP на web- серверы МСС и управления их защищенностью, так как достаточный уровень защищенности МСС различных организаций определяется приемлемым уровнем риска и управление им позволяет снизить возможные ущербы от реализации атак и сделать работу сети более стабильной, что в итоге приводит к возможности предоставлять конечным пользователям МСС более высокое качество обслуживания. Исследование информационных рисков МСС и управление их защищенностью дало следующие результаты:

1. Построенная риск-модель для web-серверов МСС, при реализации на них атак типа «отказ в обслуживании» по протоколу HTTP, основана на статистике ущербов, получена как с исследованием огибающей функции риска, так и с использованием дискретного подхода к оценке риска, что позволяет определить уровень риска в конкретный момент времени и в заданном временном интервале, с учетом специфики реализации рассматриваемых атак, физических характеристик web-серверов и связанных с ними сетевых устройств МСС. Данная модель может быть адаптирована для различных флуд-атак, реализуемых в отношении МСС.
2. Разработанная методика управления риском атакуемых web-серверов МСС описывает параметры, которыми возможно управлять, учитывает влияние изменений этих параметров на другие физические характеристики МСС, а также на формулу движения функции риска и ее абсолютные значения, что позволяет разрабатывать объективные методы по управлению риском реализации атак типа «отказ в обслуживании» по протоколу HTTP в данных системах и добиваться необходимого его уровня на атакуемом сервере. Данная методика может быть использована и для других сетевых структур.
3. Предложенная оценка эффективности защиты web-серверов МСС, подвергающихся атакам типа «отказ в обслуживании» по протоколу HTTP, позволяет оценить эффективность защиты конкретного сервера как в фиксированный момент времени, так и в заданном временном интервале. Вероятностные подходы, использованные при получении данных оценок, применимы для систем различного характера.

Применение предлагаемых в работе методик позволит создать научно­методическую основу для эффективного функционирования МСС, а также существенно снизить риски реализации и ущербы, возникающие в результате проведения атак типа «отказ в обслуживании» по протоколу HTTP на web- серверы МСС.

>

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Абрамова, Т.В. Моделирование сетевых атак на ресурсы вычислительных систем с использованием принципов самоорганизации [Текст] / Т.В. Абрамова, Т.З. Аралбаев // Сборник трудов конференции «Современные информационные технологии в науке, образовании и практике». - Оренбург: ООО ИГЖ Университет. -2014. - С. 109-114.
2. Абрамович М., Справочник по специальным функциям с формулами, графиками и таблицами [Текст] / М. Абрамович, И.Стиган. - М.: Наука. Главная редакция физико-математической литературы, 1979. - 832 с.
3. Аверченков, В.И. Автоматизация проектирования комплексных систем защиты информации [Текст] / В.И. Аверченков, М.Ю. Рытов // Информация и безопасность. - 2007. - Т. 10. - Вып. 4. - С. 582-584.
4. Адрианов, В.В. Обеспечение информационной безопасности бизнеса [Текст] / В.В. Адрианов, C.JT. Зефиров, В.Б. Голованов, Н.А. Голдуев. - М.: ЦИПСиР, 2011.-373 с.
5. Акинин, И.В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике [Текст] / И.В. Акинин // Информация и безопасность. -2014. - Т. 17. - Вып. 3. - С. 468-471.
6. Алферов, А.П. Основы криптографии [Текст] / А.П. Алферов, A.IO. Зубов, А.С. Кузьмин, А.В. Черемушкин - М.: Гелиос АРВ, 2002. - 480 с.
7. Андронов, А.М. Теория вероятностей и математическая статистика: Учебник для вузов [Текст] / А.М. Андронов, Е.А. Копытов, Л.Я. Гринглаз. - СПб.: Питер, 2004. - 461 с.
8. Белов, Е.Б. Основы информационной безопасности. Учебное пособие для вузов [Текст] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов - М.: Горячая линия-Телеком, 2006. - 544 с.
9. Белоножкин, В.И. Информационные аспекты противодействия терроризму [Текст]: монография / В.И. Белоножкин, Г.А. Остапенко. - Москва: Горячая линия-Телеком, 2009. - 112 с.
10. Бочаров, П.П. Теория вероятностей. Математическая статистика [Текст] / П.П. Бочаров, А.В. Печинкин. - М.: ФИЗМАТЛИТ, 2005. - 296 с.
11. Бутузов, В.В. К вопросу обоснования функции ущерба атакуемых систем [Текст] / В.В. Бутузов, А.В. Заряев // Информация и безопасность. - 2013. -Т. 16.-Вып. 1.-С. 47-54.
12. Васильев, В.И. Интеллектуальные системы защиты информации: учеб. пособие [Текст] / В.И. Васильев. - М.: Машиностроение, 2012. - 171 с.
13. Величко, В.В. Телекоммуникационные системы и сети: Учебное пособие в 3 томах. Том 3. - Мультисервисные сети [Текст] / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; под ред. Профессора В.П. Шувалова. - М.: Горячая линия-Телеком, 2005. -592 с.
14. Гмурман, В.Е. Теория вероятностей и математическая статистика: Учеб. Пособие для вузов [Текст] / В.Е. Гмурман. - М.: Высш. Шк., 2003. - 479 с.
15. ГОСТ Р 50922-2006. Защита информации. Основные термины и

определения. - М.: Стандартинформ. - 2008.

1. ГОСТ Р 51583-2000. Защита информации. Порядок создания

автоматизированных систем в защищенном исполнении. Общие положения. - М.: Стандартинформ. - 2008.

1. ГОСТ Р 51624-2000. Защита информации. Автоматизированные

системы в защищенном исполнении. Общие требования. - М.: Стандартинформ. - 2008.

1. ГОСТ Р 51897-2001 Менеджмент риска. Термины и определения. -

М.: Стандартинформ, 2012.

1. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска

технологических систем. - М.: Изд-во стандартов, 2002.

1. ГОСТ Р 51901.12-2007 Менеджмент риска. Метод анализа видов и

последствий отказов. - М.: Изд-во стандартов, 2007.

1. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология.

Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. - М.: Стандартинформ. - 2008.

1. Громов, IO.IO. Классификация видов атакующих воздействий на информационную систему [Текст] / 10.10. Громов, В.О. Драчев, В.В. Войтюк, Ю.Ф. Мартемьянов, АЛО. Громов // Информация и безопасность, 2010. - Т. 10. - Вып. 3.-С. 413-418.
2. Громов, 10.10. Использование теории возможностей при оценке

живучести сетевых информационных структур [Текст] / 10.10. Громов, А.А.

Долгов, М.А. Хорохорин, 10.10. Мишин // Информация и безопасность, 2014. - Т. 17. - Вып. 1.-С. 62-67.

1. Грушо, А.А Теоретические основы защиты информации [Текст] / А.А. Грушо, Е.Е. Тимонина-М.: Яхтсмен, 1996. -187 с.
2. Губанов Д.А. Социальные сети: модели информационного влияния,

управления и противоборства: под ред. чл.-корр. РАН Д.А. Новикова [Текст] /Д.А.

Губанов, Д.А. Новиков, А.Г. Чхартишвили. - М.: ФИЗМАТ, 2010. -228 с.

1. Гургенидзе, А.Т. Мультисервисные сети и услуги широкополосного доступа [Текст] / А.Т. Гургенидзе, В.И. Кореш. - М.: Экмос, 2004. - 400 с.
2. Ершов, В.А. Мультисервисные телекоммуникационные сети [Текст] /

В.А. Ершов, Н.А. Кузнецов. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2003. - 432 с.

1. Зегжда, П.Д. Основы информационной безопасности: монография [Текст] / П.Д. Зегжда, Е.А. Рудина. - СПб.: Изд-во Политехи, ун-та, 2008. - 224 с.
2. Иванкин, Е.Ф. Инновационные платежные системы на основе банковских карт: методы снижения информационных рисков [Текст] / Е.Ф. Иванкин, М.М. Жуков, Р.В. Менжулин // Информация и безопасность. - 2012. - Т.
3. - Вып. 3.-С. 299-312.
4. Калашников А.О. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков [Текст]: монография / А.О. Калашников, Е.В. Ермилов, О.Н. Чопоров, К.А. Разинкин, Н.И. Баранников; под ред. чл.-корр. РАН Д.А. Новикова. - Воронеж: Научная книга. 2013. 160 с.
5. Калашников, А.О. Модели и методы организационного управления информационными рисками корпораций / А.О. Калашников. - М: Эгвес, 2011. - 312 с.
6. Карпеев, Д.О. Анализ и управление рисками: исследование в контексте обеспечения безопасности информационных систем [Текст] / Д.О. Карпеев // Современные информационные технологии в науке, образовании и практике: материалы VI Всерос. науч.-практ. конф. (с междунар. участием). - Оренбург: ИПК ГОУ ОГУ, 2007. - С. 306-307.
7. Карпеев, Д.О. Стратегии управления рисками в социотехнических информационных системах [Текст] / Д.О. Карпеев, Г.А. Остапенко, В.И. Белоножкин // Информация и безопасность: региональный научно-технический журнал - Воронеж, 2006. - Вып. 2. - С. 133-134.
8. Козачок, В.И. Особенности разработки распределенных систем обнаружения компьютерных атак для высокоскоростных сетей связи [Текст] /
9. И. Козачок, А.Г. Мацкевич, С.В. Морковин // Информация и безопасность. - 2014. - Т. 17 - Вып. 2-С. 236-239.
10. Ланкин, О.В. Оценка качества информационной деятельности в

условиях обеспечения защищенности речевой информации [Текст] / О.В. Ланкин,

1. Ю. Рослов, А.В. Любченков // Информация и безопасность. - 2014. - Т. 17 - Вып.4 — С. 618-622.
2. Малюк, А.А. Теория защиты информации. Монография [Текст] / А.А. Малюк - М.: Горячая линия-Телеком, 2012. -184 с.
3. Меньших В.В. Моделирование возникновения угроз информационной безопасности на объекте информатизации [Текст] /В.В. Меньших, О.В. Толстых // Информация и безопасность, 2011.-Т. 14.-Вып. 1.-С. 117-120.
4. Минаев, В.А. Основы информационной безопасности: Учебник

[Текст] / В.А. Минаев, С.В. Скрыль, А.П. Фисун, В.Е. Потанин, С.В. Дворянкин. - Воронеж: Воронежский институт МВД России, 2000. - 464 с.

1. Новиков Д.А. Управление информационными рисками в

инновационной России [Текст] / Д.А. Новиков, А.О. Калашников // Информация и безопасность. -2013. -Т.16. -№ 3. - С. 319-322.

1. Новиков, Д.А. Прикладные модели информационного управления [Текст] / Д.А. Новиков, А.Г. Чхартишвили - М.: Институт проблем управления им. В.А. Трапезникова РАН, 2004. - 129 с.
2. Носов, JT.C. Оценка защищённости СВТ путём моделирования канала ПЭМИН [Текст] / Л.С. Носов // Математические структуры и моделирование. -

2014.-№4-С. 254-257.

1. Остапенко А.Г. Жизнестойкость атакуемых распределенных систем: оценка рисков фатальных отказов компонентов [Текст]: монография / А.Г. Остапенко, Д.Г. Плотников, O.IO. Макаров, Н.М. Тихомиров, В. Г. Юрасов; под ред. чл.-корр. РАН Д.А. Новикова. - Воронеж: Научная книга, 2013. - 160 с.
2. Остапенко А.Г. Риск-анализ информационно-телекоммуникационных систем, подвергающихся атакам типа «сетевой шторм» [Текст]: монография / А.Г. Остапенко, С.С. Куликов, Н.Н. Толстых, Ю.Г. Пастернак, Ю.Е. Дидюк; под ред. чл.-корр. РАН Д.А. Новикова. - Воронеж: Научная книга, 2013. - 160 с.
3. Остапенко, А.Г. К вопросу об управлении рисками распределенных информационных систем [Текст] / А.Г. Остапенко, Д.Г. Плотников, АЛО. Дуплищева // Информация и безопасность. - 2010. - Т. 13. - Вып. 2. - С. 259-260.
4. Остапенко, А.Г. Функция возможности в оценке рисков, шансов и эффективности систем [Текст] / А.Г.Остапенко // Информация и безопасность. - 2010.-Т. 13.-Вып. 1.-С. 17-20.
5. Остапенко Г.А. Концептуальный подход к расчету и регулированию рисков нарушения актуальности информации в элементах критической информационной инфраструктуры [Текст] / Г.А. Остапенко, А.Н. Шершень, А.О. Калашников // Информация и безопасность. -2013. - Т. 16. — № 2. - С. 239-242.
6. Остапенко, Г.А. Информационные операции и атаки в социотехнических системах [Текст]: монография / Г.А. Остапенко; под ред. В.И. Борисова. - М.: Горячая линия-Телеком. 2006. - 134 с.
7. Остапенко, Г.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия [Текст]: Учебное пособие / А. Г. Остапенко, Е.А. Мешкова. - М: Горячая линия- Телеком, 2007. - 295 с.
8. Остапенко Г.А. Информационные риски в социальных сетях / Г.А. Остапенко, Л.В. Паринова, В.И. Белоножкин, И.Л. Батаронов, К.В. Симонов / Под ред. член-корр. РАН Д.А. Новикова. 2013. 161с.
9. Остапенко, Г.А. К вопросу об оценке ущерба и жизнестойкости атакуемых распределенных информационных систем: развитие методического обеспечения [Текст] / Г.А. Остапенко, Д.Г. Плотников, НЛО. Щербакова, B.C. Зарубин//Информация и безопасность.-2013.-Т. 16.-Вып. 1.-С. 141-142.
10. Остапенко, Г.А. Способы регулирования рисков распределенных систем [Текст] / Г.А. Остапенко, П.А. Маслихов, Е.В. Субботина // Информация и безопасность. - 2010. -Т. 13. -Вып. 3.-С. 435-438.
11. Остапенко, Г.А. Управление информационными рисками распределенных систем: актуальные направления исследований [Текст] / Г.А. Остапенко, В.И. Борисов // Системы управления и информационные техонологии: научный технический журнал. М., 2011. - Вып. 1. - С. 163-167.
12. Остапенко, О. А. Динамическая постановка задачи оценки и управления рисками [Текст] / О.А. Остапенко, Д.О. Карпеев // Инновации, риски, безопасность: межрегион. науч.-практ. конф. - Воронеж: МИКТ, 2008. С. 67-68.
13. Попов, Г.А. Модель анализа эмпирических данных в системах безопасности [Текст] / Г.А. Попов // Вестник Астраханского государственного технического университета. - 2010. -Вып. 1. - С. 54-61.
14. Попов, Е.А. Спам-атаки на распределенные автоматизированные системы: аналитическое выражение ущерба [Текст] / Попов Е.А., Чопоров О.Н., Попова Л.Г., Остапенко О.А. // Информация и безопасность. - 2014. - Т. 17. - Вып. 4. - С. 634-637.
15. Радько, Н.М. Методический подход к определению эпистойкости автоматизированной информационной системы (АИС), атакуемой вирусами [Текст] / Радько Н.М., Теслинов В.А., Толстых Н.Н. // Информация и безопасность. - 2014. - Т. 17. - Вып. 2. - С. 252-255.
16. Радько, Н.М. Некоторые оценки рисков, шансов и живучести сетей в условиях информационных атак вирусного характера [Текст] / Радько Н.М.,

Паринова JT.B., Пастернак Ю.Г., Разинкин К.А., Тихомиров Н.М. // Информация и безопасность. - 2013. - Т. 16. - Вып. 4. - С. 498-499.

1. Радько, Н.М. Оценка отказоустойчивости узлов автоматизированных систем и доступности информации: статистический риск-анализ и управление защищенностью [Текст] / Н.М. Радько, Д.М. Фурсов, Д.А. Андреев // Информация и безопасность. - 2007. -Т. 10. - Вып. 2. - С. 359.
2. Радько, Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа [Текст]: монография / Н.М. Радько, И.О. Скобелев. - Москва: РадиоСофт. 2010. - 232 с.
3. Радько, Н.М. Тотальные вирусные атаки на распределенные информационные системы: обобщенные модели оценки рисков возникновения эпидемий и шансов эффективного противодействия им [Текст] / Радько Н.М., Паринова JI.B., Пастернак Ю.Г., Разинкин К.А., Тихомиров Н.М. // Информация и безопасность. -2013. - Т. 16. - Вып. 4.-С. 500-501.
4. Сайт компании «Akamai» [Электронный ресурс]. - Режим доступа: <http://www.akamai.com>.
5. Сайт компании «Arbor Networks» [Электронный ресурс]. - Режим доступа: [http://www.arbornetworks.com.](http://www.arbornetworks.com)
6. Сайт компании «Cisco Systems» [Электронный ресурс]. - Режим доступа: [http://www.cisco.com.](http://www.cisco.com)
7. Сайт компании «ESET» [Электронный ресурс]. - Режим доступа: <http://www.esetnod32.ru>.
8. Сайт компании «McAfee» [Электронный ресурс]. - Режим доступа: <http://www.mcafee.com>.
9. Сайт компании «Microsoft» [Электронный ресурс]. - Режим доступа: <http://www.microsoft.com>.
10. Сайт компании «Panda Security» [Электронный ресурс]. - Режим доступа: [http://www.pandasecurity.com.](http://www.pandasecurity.com)
11. Сайт компании «Positive Technologies» [Электронный ресурс]. - Режим доступа: [http://www.securitylab.ru.](http://www.securitylab.ru)
12. Сайт компании «Prolexic Technologies» [Электронный ресурс]. - Режим доступа: [http://www.prolexic.com.](http://www.prolexic.com)
13. Сайт компании «Radware» [Электронный ресурс]. - Режим доступа: <http://security.radware.com>.
14. Сайт компании «Symantec Corporation» [Электронный ресурс]. - Режим доступа: [http://www.symantec.com.](http://www.symantec.com)
15. Сайт компании «Лаборатория касперского» [Электронный ресурс]. - Режим доступа: [http://www.kaspersky.ru.](http://www.kaspersky.ru)
16. Сайт сообщества Internet Engineering Task Force [Электронный ресурс]. - Режим доступа: [https://www.ietf.org.](https://www.ietf.org)
17. Степанов, С.Н. Основы телетрафика мультисервисных сетей [Текст] /

С.Н. Степанов. - М.: Эко-Трендз, 2010. - 394 с.

1. Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы [Текст] / А.А. Стрельцов; под. ред.

В.А. Садовничего и В.П. Шестюка. - М.: МЦНМО, 2002. -296 с.

1. Студенников, К.О. Исследование зависимостей информационного риска от параметров байесовской сети [Текст] / К.О. Студенников, В.Н. Лопин // Информация и безопасность. - 2013. - Т. 16. - Вып. 3. - С. 419-422.
2. Тарасов, А.А. Функциональная реконфигурация отказоустойчивых систем. Монография [Текст] / А.А. Тарасов - М.: Логос, 2012.- 152 с.
3. Тарасов, Я.В. Моделирование и исследование низкоинтенсивных DOS-атак на BGP-инфраструктуру [Текст] / Я.В. Тарасов, О.Б. Макаревич // Известия Южного федерального университета. Технические науки. -2013. -№12. -С. 101-111.
4. Тишков, С.А. Актуальность риск-анализа компьютерных систем при отказах в обслуживании [Текст] / С.А. Тишков, Р.В. Батищев // Современные информационные технологии в науке, образовании и практике. Материалы VII Всерос. науч.-практ. конф. с междунар. участием. - Оренбург, 2008. - С. 154-155.
5. Тишков, С.А. Динамические модели риска отказов в обслуживании [Текст] / С.А. Тишков, А.Г. Остапенко // Информация и безопасность. - 2008. - Т. И. -Вып. 4.-С. 609-610.
6. Тишков, С.А. Исследование возможностей регулирования рисков автоматизированных систем при защите от атак типа «отказ в обслуживании» [Текст] / С.А. Тишков // Информация и безопасность. - 2009. - Т. 12. - Вып. 1. -

С. 25-38. .

1. Тишков, С.А. Концепция риск-анализа отказов в обслуживании

автоматизированных систем [Текст] / С.А. Тишков // Информация и безопасность. -2008. -Т. 11. -Вып. 4.-С. 623.

1. Тишков, С.А. Обобщенная постановка задачи стохастического

моделирования отказов в обслуживании для автоматизированных систем [Текст] /

С.А. Тишков // Информация и безопасность. - 2008. - Т. 11. - Вып. 3. - С. 469.

1. Тишков, С.А. Риск-модели распределенных атак отказа в

обслуживании [Текст] / С.А. Тишков // Информация и безопасность. - 2008. - Т.

1. -Вып. 4.-С. 613-614.
2. Филимонов, АЛО. Построение мультисервисных сетей Ethernet [Текст] / АЛО. Филимонов. - СПб.: БХВ-Пет ербург, 2007. - 592 с.
3. Цыбуля, С.В. Введение в структурный анализ нанокристаллов: учеб. пособие [Текст] / С.В. Цыбуля, С.В. Черепанова - Новосибирск: ФГБОУ ВПО «Новосибирский государственный университет», 2008. - 92 с.
4. Шишкин, Н.В. Алгоритм обнаружения вредоносных программ на основе анализа их поведения [Текст] / Н.В. Шишкин, Мацкевич Е.Е., Козачек А.В. // Информация и безопасность. - 2012. - Т. 15. - Вып. 3. - С. 353-360.
5. Щербаков, В.Б. Безопасность беспроводных сетей: стандарт IEEE 802.11 [Текст]: монография / В.Б. Щербаков, С.А. Ермаков. - Москва: РадиоСофт, 2010.-255 с.
6. Щербаков, В.Б. Риск-анализ атакуемых беспроводных сетей [Текст]: монография/ В.Б. Щербаков, С.А. Ермаков, Н.С. Коленбет; под ред. чл.-корр. РАН Д.А. Новикова. — Воронеж: Научная книга, 2013. - 160с.
7. Юрасов, В.Г. Построение матрицы чувствительности рисков для субъектов социальной информационной сети [Текст] / Юрасов В.Г., Коваленко Д.М., Остапенко Г.А., Баленко М.А. // Информация и безопасность. - 2011. - Т.
8. - Вып. 3.-С. 401-408.
9. Язов Ю.К. Метод формализации процесса несанкционированного доступа в ИС, построенных с использованием средств виртуализации, основанный на математическом аппарате сетей Петри [Текст] / Ю.К. Язов, А.В. Бабурин // Информация и безопасность. -2013. -Т.16. -№ 4. -С. 518-522.
10. Butuzov V.V. Email-flooder attacks: The estimation and regulation of damage / V.V. Butuzov, A.G. Ostapenko, P.A. Parinov, G.A. Ostapenko // Life Science Journal.-2014.- 11 (7s). - P. 213-218.
11. Deshina A.E. Approach to parametric synthesis of a multiserver system with predefined risk / A.E. Deshina, A.G. Ostapenko, G.A. Ostapenko, I.A. Ushkin // Life Science Journal. - 2014. - 11 (12). - P. 390-393.
12. Ermakov S.A. Optimization of expert methods used to analyze information security risk in modem wireless networks / S.A. Ermakov, N.S. Kolenbet, A.G. Ostapenko, A.O Kalashnikov, A.S. Zavorykin // Life Science Journal. - 2014. - 23 (9). -P. 1239-1244.
13. Kalashnikov A.O. Ensuring the security of critically important objects and trends in the development of information technology / A.O. Kalashnikov, Y.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov // World Applied Sciences Journal. - 2013. - № 25 (3). - P. 399-403.
14. Mirkovic, J. A taxonomy of DDoS attack and DDoS defense mechanisms / Jelena Mirkovic, Peter Reiher // ACM SIGCOMM Computer Communication Review Volume 34 Issue 2, 2004, pp. 39-53.
15. Ostapenko A.G. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. -2013.-25 (3). - P. 404-409.
16. Ostapenko A.G. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. -2013.-25 (4). - P. 675-679. •
17. Ostapenko G.A. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y

Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. - 2013. -25 (3).-P. 416-420.

1. Ostapenko G.A. Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. - 2013. -25 (3).-P. 410-415.
2. Radko N.M. Peak Risk Assessing The Process of Information Epidemics / Expansion N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences biotechnology research Asia. - November, 2014. - Vol.l 1 (Spl. Edn.). - P. 251-255.

**Основные результаты диссертации опубликованы в следующих работах: Публикации в изданиях, рекомендованных перечнем ВАК РФ**

1. Остапенко, Г.А. Информационные ресурсы инновационных проектов: риск-моделирование в условиях DDoS-атак [Текст] / Г.А. Остапенко, М.В. Бурса, Е.А. Попов, С.С. Вяхирева // Информация и безопасность. - 2012. - Т. 15. - Вып.

З.-С. 345-352.

1. Остапенко, Г.А. Аналитическое моделирование процесса реализации ddos-атаки типа HTTP-flood [Текст] / Г.А. Остапенко, М.В. Бурса, Е.Ф. Иванкин //Информация и безопасность. - 2013. - Т. 16.-Вып. 1.-С. 107-110.
2. Бурса, М.В. DDoS-атаки на информационно-телекоммуникационные системы: управление рисками [Текст] / М.В. Бурса, Ю.Г. Пастернак // Информация и безопасность. - 2013. - Т. 16. - Вып. 2. - С. 255-256.
3. Остапенко, Г.А. Риск-модель инновационного проекта, функционирующего в условиях угроз реализации DDoS-атак [Текст] / Г.А. Остапенко, М.В. Бурса, Н.Н. Толстых // Информация и безопасность. - 2013. - Т.
4. -Вып. З.-С. 443-444.
5. Остапенко, Г.А. Оценка защищенности ресурсов информационно­телекоммуникационных систем, подвергающимся DDoS-атакам [Текст] / Г.А.

Остапенко, М.В. Бурса, Н.И. Баранников, И.Л. Батаронов // Информация и безопасность. - 2013. - Т. 16. - Вып. 4. - С. 496-497.

1. Бурса, М.В. Обоснование выбора функции ущерба атаки типа «НТТР- флуд» [Текст] / М.В. Бурса, Д.О. Бутрик // Информация и безопасность. - 2014. — Т. 17.-Вып. 1.-С. 104-107.
2. Бурса, М.В. Аналитическая оценка пика функции риска для компонентов информационно-телекоммуникационных систем, подвергающимся атакам типа НТТР-флуд [Текст] / М.В. Бурса // Информация и безопасность. - 2014. - Т. 17. - Вып. 2. - С. 232-235.
3. Бурса, М.В. НТТР-флуды информационно-телекоммуникационных систем: оценка рисков и управление защищенностью [Текст] / М.В. Бурса, А.Г. Остапенко, А.О. Калашников // Сборник трудов конференции «XII всероссийское совещание по проблемам управления ВСПУ-2014» Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 9150-9153.
4. Бурса, М.В. Оценка риска реализации распределенных атак типа «НТТР-флуд» на многокомпонентные информационно-телекоммуникационные системы [Текст] / М.В. Бурса, Г.А. Остапенко // Информация и безопасность. - 2014. - Т. 17. - Вып. 3. - С. 424^27.
5. Остапенко, Г.А. Дискретная риск-модель: выбор шага дискретизации для оценки риска и оценка возможной эффективности компонентов информационно-телекоммуникацоинных систем при реализации на них атак типа «НТТР-флуд» [Текст] / Г.А. Остапенко, М.В. Бурса, Н.М. Тихомиров // Информация и безопасность. - 2014. - Т. 17. - Вып. 4. - С. 592-597.

**Книги**

1. Дешина А.Е. Управление информационными рисками мультисерверных систем при воздействии DDoS-атак: монография [Текст] / А.Е. Дешина, М.В. Бурса, А.Г. Остапенко, А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. - Воронеж: Научная книга, 2014.- 160 с.
2. Бутузов В.В. Информационные риски флуд-атакуемых компьютерных систем: монография [Текст] / В.В. Бутузов, М.В. Бурса, А.Г. Остапенко, А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. - Воронеж: Научная книга, 2015. - 160 с.
3. Остапенко А.Г. Математические основы риск-анализа: учеб. пособие [Электронный ресурс] / А.Г. Остапенко, М.В. Бурса.- Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013.

**Статьи и материалы конференций**

1. Бурса, М.В. Подход к управлению рисками информационно­телекоммуникационной системы для гамма-распределения плотности вероятности наступления ущерба [Текст] / М.В. Бурса // Труды Всероссийской научно-технической конференции «Перспективные исследования и разработки в области информационных технологий и связи». - 2013. - С. 18.
2. Бурса, М.В. Параметры риска в информационно­телекоммуникационных системах, подвергающихся распределенным атакам типа «отказ в обслуживании» [Текст] / М.В. Бурса // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. -2013. - Вып. 1. - С. 135-145.
3. Бутрик, Д.О. Модели реализации распределенных атак типа НТТР- flood на основе аппарата сетей Петри-Маркова [Текст] / Д.О. Бутрик, М.В. Бурса // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. -2013. - Вып. 2 - С. 138-157.
4. Бурса, М.В. Моделирование DDoS-атак типа «НТТР-флуд» на сетевые структуры [Текст] / М.В. Бурса, Д.О. Бутрик // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. - 2014. - Вып. 1 - С. 51-70.
5. Бурса, М.В. Управление риском ресурса информационно­телекоммуникационной системы, подвергающейся атакам типа «НТТР-флуд» с

точки зрения физических возможностей реального оборудования / М.В. Бурса, АЛО. Мещерякова // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. - 2014. - Вып. 3 - С. 103-120.

1. Бурса, М.В. Атаки типа «НТТР-флуд» на компоненты информационно-телекоммуникационных систем: оценка максимального значения риска / М.В. Бурса, Г.А. Остапенко // Труды Всероссийской научно-технической конференции «Перспективные исследования и разработки в области информационных технологий и связи». - 2014. - С. 60.
2. Бурса, М.В. Атаки типа «НТТР-флуд»: аналитическое обоснование функции ущерба от их реализации / М.В. Бурса, П.С. Воронов, А.А. Остапенко, Р.К. Бабаджанов // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. - 2014. - Вып. 4 - С. 29-38. •
3. Бурса, М.В. Аналитическая оценка ущерба и риска реализации атак типа «НТТР-флуд» на мультисервисные сети / М.В. Бурса, Г.А. Остапенко // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. -2014. - Вып. 4 - С.71 -99.
4. Калашников, А.О. Мультисервисные сети: дискретная риск-модель НТТР-флуда / А.О. Калашников, М.В. Бурса, Г.А. Остапенко // Вопросы кибербезопасности . - 2015. - Вып. 1. - С. 49-54.

**Публикации в изданиях по перечню SCOPUS**

1. Ostapenko A.G. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences biotechnology research Asia. - 2014. - Vol. 11 (Spl.Edn.).- P.173-176.