

**Содержание:**

<b>Студенческая конференция по проблемам компьютерной безопасности</b> «IT-Security Conference for the Next Generation» .....	3
<b>Организационный комитет</b> .....	4
<b>Итоги конференции</b> .....	5
<b>Медиация - приоритетный выбор альтернативного метода при разрешении внутри -</b> <b>межкорпоративных споров Theme: Mediation – privileged accommodation of corporate disputes</b> <b>(inside the company and between companies).</b> Архипов Максим Витальевич Arkhipov Maxim .....	8
<b>Безопасность «облачных» технологий в современных провайдерских сетях</b> Баринов А.Е.....	9
<b>Информационно-образовательный портал по правовым аспектам защиты информации «LIS-</b> <b>Russia.NET»</b> Авторы: Бедиров Мурад Рамазанович .....	10
Пацукова Валентина Сергеевна, Чичиков Анатолий Александрович .....	10
<b>Система обнаружения неизвестных вредоносных</b> .....	11
<b>программ в корпоративной сети по анализу подозрительных действий</b> Авторы: Бердник Владимир Александрович, Цветков Максим Витальевич .....	11
<b>Повышение эффективности противодействия сетевым угрозам посредством интеграции</b> <b>технологий</b> .....	13
Дугин Андрей Олегович .....	13
<b>Оценка количества людей, имеющих персональные данные в открытом доступе (на примере</b> <b>города Магнитогорска)</b> Калиновский Евгений Александрович .....	15
<b>Автоматическое детектирование новых вредоносных программ на базе структурной</b> <b>информации о PE-файле</b> Кипер Андрей Борисович Ляшенко Елизавета Владимировна.....	16
<b>Анализ стратегий защиты цифровых программных продуктов от интернет-пиратства с</b> <b>использованием метода экономико-математического моделирования</b> Автор Лаушкин Алексей Николаевич.....	17
<b>Детектирование вредоносных соединений методом нейронных карт</b> Кохонена Миникаев Ришат Фаритович.....	19
<b>ИНФРАСТРУКТУРА ДИАГНОСТИРОВАНИЯ СПАМА В ИНДИВИДУАЛЬНОМ КИБЕРНЕТИЧЕСКОМ</b> <b>ПРОСТРАНСТВЕ</b> Мищенко А.С., Хаханова Ю.В.....	22
<b>Особенности использования метода case-study при преподавании информационной</b> <b>безопасности</b> Савельева А.А. ....	23
<b>Международная защита интеллектуальной собственности в сфере компьютерных технологий</b> Титова Мария Александровна .....	26
<b>Обнаружение аномалий сети на основе вейвлет-пакетов и ARX-модели</b> Тишина Н.А.....	27
<b>Методика обеспечения безопасности ведения сайтов образовательных учреждений</b> Топчий Андрей Константинович .....	29
<b>Учебный проект для обучения студентов гуманитарных специальностей навыкам</b> <b>обеспечения защиты информации</b> Филимошин В. Ю.....	31
<b>Интеллектуальная фильтрация несанкционированных рассылок на основе нейронной сети</b> Чернопрудова Елена Николаевна .....	32

# Студенческая конференция по проблемам компьютерной безопасности «IT-Security Conference for the Next Generation»

## Цель конференции:

Объединить специалистов, молодых ученых, исследователей, изучающих проблемы компьютерной безопасности для обмена опытом, развития инноваций и повышения уровня безопасности в сфере информационных технологий. Обеспечить поддержку молодых ученых для развития исследований в области ИБ.

## Даты проведения:

**Заочный тур:** 01 сентября 2011 г. – 14 февраля 2011 г.

**Оценка работ** программным комитетом: до 11 февраля 2011 года

**Очный тур:** 9-11 марта 2011 г., г. Москва, факультет Вычислительной Математики и Кибернетики Московского Государственного Университета

**Организаторы:** ЗАО «Лаборатория Касперского», факультет ВМиК МГУ.

## Темы конференции:

### Технические номинации

- Тенденции развития анти-спам технологий, методы спамовой "гонки вооружений", инновационные решения для защиты от спама.
- Сетевые угрозы в условиях современной компьютеризации мира.
- "Облачные" технологии безопасности.
- Технологии будущего для обнаружения и борьбы с вредоносным ПО (например, искусственный интеллект, нечеткие системы, сети p2p и т.д.).

### Социальные, экономические и правовые

- Информационная защита общества в современных условиях (например, безопасность социальных сетей, встроенные системы безопасности, безопасность мобильных устройств, защита систем онлайн-банкинга).
- Потенциальные проблемы и их решения в области информационной безопасности на ближайшие 10 лет.
- Влияние развития компьютерных технологий на проблемы защиты данных, прав копирования, интеллектуальной собственности и проблемы законодательства. Образовательные проекты по ИТ безопасности. Тенденции и вопросы

## Программный комитет

1. **Березин Борис Иванович**, кандидат физико-математических наук, зам.декана факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова
2. **Васильев Сергей Алексеевич**, аналитик по интеллектуальной собственности, ЗАО «Лаборатория Касперского».
3. **Голованов Сергей Юрьевич**, ведущий вирусный аналитик, ЗАО «Лаборатория Касперского».
4. **Гудкова Дарья Владимировна**, Руководитель отдела контентных аналитиков, ЗАО «Лаборатория Касперского».
5. **Ершов Игорь Валерьевич**, кандидат физико-математических наук, доцент, кафедра информационных систем и технологий, Новосибирский Государственный Архитектурно-строительный университет
6. **Ефимова Светлана Николаевна**, Руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского»
7. **Казмирова Екатерина Дмитриевна**, Копирайтер-редактор, ЗАО «Лаборатория Касперского»
8. **Кадиев Алексей Махаевич**, Вирусный аналитик, ЗАО «Лаборатория Касперского»
9. **Кащенко Надежда Васильевна**, Руководитель отдела по управлению интеллектуальной собственностью ЗАО «Лаборатория Касперского».
10. **Малов Антон Евгеньевич**, аналитик по интеллектуальной собственности, ЗАО «Лаборатория Касперского».
11. **Масленников Денис Игоревич**, старший вирусный аналитик, ЗАО «Лаборатория Касперского».
12. **Мельников Николай Викторович**, доктор технических наук, профессор, зав.каф. Информационной безопасности, Российский государственный социальный университет
13. **Минзов Анатолий Степанович**, доктор технических наук, профессор, зав.кафедрой «Комплексная безопасность бизнеса», Институт безопасности бизнеса Московского энергетического института (ТУ)
14. **Новиков Сергей Валерьевич**, Руководитель российского исследовательского центра ЗАО «Лаборатория Касперского».
15. **Филиппович Андрей Юрьевич**, Преподаватель кафедры АСУ (ИУ5) МГТУ им. Н.Э.Баумана
16. **Хаханов Владимир Иванович**, профессор, доктор технических наук, декан факультета компьютерной инженерии и управления, Харьковский национальный университет радиоэлектроники.
17. **Ефимова Светлана Николаевна**, Руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского»

## Организационный комитет

1. **Селезнева Ирина Анатольевна**, координатор образовательных программ ЗАО «Лаборатория Касперского»
2. **Ефимова Светлана Николаевна**, руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского».
3. **Федорова Ольга Александровна**, методист образовательных программ «Лаборатории Касперского».
4. **Горелова Анастасия Ивановна**, координатор образовательных программ ЗАО «Лаборатория Касперского»

## Итоги конференции

Лучшие работы заочного тура конференции по результатам оценки программного комитета

### Тенденции развития Анти-Спам технологий, методы "Спамовой гонки вооружений", инновационные решения борьбы со спамом.

Автор	Наименование работы	Учебное учреждение	Город, страна
Мищенко Александр; Хаханова Юлия	Инфраструктура диагностирования спама в индивидуальном кибернетическом пространстве	Харьковский национальный университет радиоэлектроники	Харьков, Украина
Чернопрудова Елена	Интеллектуальная фильтрация несанкционированных рассылок на основе нейронной сети	Оренбургский государственный университет	Оренбург, Россия

### Сетевые угрозы в условиях современной компьютеризации мира

Автор	Наименование работы	Учебное учреждение	Город, страна
Косарева Анастасия	Стохастическая модель развития вирусных эпидемий в компьютерных сетях	Московский государственный университет приборостроения и информатики	г. Дедовск, Россия
Дугин Андрей	Повышение эффективности противодействия сетевым угрозам посредством интеграции технологий	Украинский научно-исследовательский институт связи	Киев, Украина

### 'Облачные технологии' безопасности.

Автор	Наименование работы	Учебное учреждение	Город, страна
Баринев Андрей	Безопасность облачных технологий в современных провайдерских сетях	Южно-Уральский государственный университет	Челябинск, Россия

### Технологии будущего для обнаружения и борьбы с вредоносным ПО (например, искусственный интеллект, нечеткие системы, сети p2p).

Автор	Наименование работы	Учебное учреждение	Город, страна
Миникаев Ршад	Детектирование вредоносных соединений методом нейронных карт Кохонена	Московский Физико-Технический Институт	Москва, Россия
Бердник Владимир, Цветков Максим	Система обнаружения неизвестных вредоносных программ в корпоративной сети по анализу подозрительных действий	Костанайский государственный университет имени Ахмета Байтурсынова	Костанай, Казахстан
Кипер Андрей, Ляшенко	Автоматическое детектирование новых вредоносных программ на	Одесский Национальный Политехнический	Одесса, Украина

Елизавета базе структурной информации о PE- Университет, файле

**Информационная защита общества в современных условиях (например, безопасность социальных сетей , встроенные системы безопасности, безопасность мобильных устройств, защита систем онлайн-банкинг).**

Автор	Наименование работы	Учебное учреждение	Город, страна
Топчий Андрей	Методика обеспечения безопасности ведения сайтов образовательных учреждений	Южно-Уральский государственный университет	Челябинск, Россия
Тишина Наталья	Обнаружение аномалий сети на основе вейвлет-пакетов и ARX-модели	ГОУ ВПО Оренбургский государственный университет	Оренбург, Россия
Калиновский Евгений	Оценка количества людей, имеющих персональные данные в открытом доступе (на примере города Магнитогорска)	Магнитогорский государственный университет	Магнитогорск, Россия

**Влияние развития компьютерных технологий на проблемы защиты данных, прав копирования и интеллектуальной собственности, законодательства.**

Автор	Наименование работы	Учебное учреждение	Город, страна
Бедиров Мурад, Пацукова Валентина, Чичиков Анатолий	Информационно-образовательный портал по правовым аспектам защиты информации LIS-Russia.NET	Пятигорский государственный лингвистический университет	Пятигорск, Россия
Лаушкин Алексей	Анализ стратегий защиты цифровых программных продуктов от Интернет-пиратства с использованием метода экономико-математического моделирования	Донецкий национальный университет	Донецк, Украина
Титова Мария	Международная защита интеллектуальной собственности в сфере компьютерных технологий	Московский институт экономики, менеджмента и права	Москва, Россия
Архипов Максим	Медиация - приоритетный выбор альтернативного метода разрешения межкорпоративных споров	Ульяновский государственный университет	Ульяновск, Россия

**Образовательные проекты по ИТ безопасности -Тенденции и вопросы.**

Автор	Наименование работы	Учебное учреждение	Город, страна
Филимошин Вадим	Учебный проект для обучения студентов гуманитарных специальностей навыкам обеспечения защиты информации	Магнитогорский государственный университет	Магнитогорск, Россия

Гулакова Анастасия	Учебный проект "Родительский контроль"	Магнитогорский государственный университет	Магнитогорск, Россия
Савельева Александра	Особенности использования метода case-study при преподавании информационной безопасности	Государственный университет - Высшая школа экономики	Москва, Россия
Рындин Артём	Учебный проект для учащихся 10-11 классов по авторскому праву в Интернете	Магнитогорский государственный университет	Магнитогорск, Россия

## **Медиация - приоритетный выбор альтернативного метода при разрешении внутри - межкорпоративных споров**

### **Theme: Mediation – privileged accommodation of corporate disputes (inside the company and between companies).**

**Архипов Максим Витальевич**  
**Arkhipov Maxim**

**Ульяновский государственный университет**

**Ульяновск, Россия**

**Ulyanovsk social university**

[annya\\_annya@mail.ru](mailto:annya_annya@mail.ru)

This article is about the mediation which is the alternative (not judicial) method of solving different disputes. Mediation also helps to solve the corporate disputes and IT security.

В экономике современных государств главенствующая роль принадлежит корпоративным организациям. Наблюдается некая тенденция поглощения небольших коммерческих структур более крупными организациями, влекущая обострение корпоративных конфликтов, как внутренних, так и межкорпоративных.

Появились современные новые формы и способы нарушения корпоративных прав, новые виды соответствующих правонарушений, в том числе связанных с защитой данных. В свою очередь, это требует установления адекватных и доступных средств защиты корпоративных прав и интересов, разработки гражданско-правового инструментария для формирования механизма защиты корпоративных прав и интересов.

Для крупных и успешных компаний уже давно не является исключением наличие в контрактах (как трудовых, так и на оказание различного рода услуг) параграфов и глав касающихся защиты данных и коммерческой тайны.

Споры, возникающие из корпоративных правоотношений, были переданы в исключительную компетенцию арбитражных судов, но применение только такой формы защиты, к сожалению, является малоэффективной.

Включение корпоративных правоотношений в сферу гражданских правоотношений обуславливает необходимость исследования вопросов, связанных с применением предусмотренных гражданским законодательством способов защиты для защиты корпоративных прав и интересов.

Специфика содержания корпоративных правоотношений, формы корпоративных правонарушений определяют и особенности гражданско-правовой защиты прав и интересов участников названных правоотношений.

Безусловно, заинтересованные лица могут прибегнуть к судебной защите посредством иска, если ущерб уже причинен, но возместить его в судебном порядке все равно в полном объеме не удастся. В связи с этим появилась необходимость нормативного регулирования и распространения альтернативных способов разрешения корпоративных споров, одним из которых является медиация (посредничество).

Деловое сообщество как наиболее активная и открытая ко всему новому часть общества должна стать одной из ведущих сил, способствующих внедрению медиации (посредничества) в российскую правовую культуру, исходя из того, что медиация как альтернативный метод разрешения споров отвечает потребностям участников экономической и хозяйственной деятельности, создавая условия для безопасного и стабильного ведения бизнеса.

Полномасштабное развитие альтернативных методов разрешения споров возможно лишь при поддержке государства, законодательной, исполнительной и судебной власти. Эта помощь должна выражаться во всестороннем содействии развитию института медиации (посредничества) как одного из важных элементов гражданского общества и создания необходимой нормативной и законодательной базы по применению альтернативных методов разрешения споров, и в частности, медиации (посредничества) в Российской Федерации.

Медиация является удобным, современным и эффективным способом разрешения корпоративных споров, в том числе и в сфере информационной безопасности

## Безопасность «облачных» технологий в современных провайдерских сетях

Баринов А.Е.

Южно-уральский государственный университет  
Челябинск, Россия

Облачные вычисления - технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис.

На сегодняшний день облачные вычисления реализованы на трёх уровнях виртуализации: программное обеспечение как услуга (Software as a Service, SaaS), платформа как услуга (Platform as a Service, PaaS) и инфраструктура как услуга (Infrastructure as a Service, IaaS). SaaS подразумевает аренду уже готовых бизнес-приложений, прежде всего в таких областях, как CRM (система управления взаимодействием с клиентами), совместную работу над проектами и прочее. Следующий уровень – PaaS – более низкоуровневые сервисы: базы данных, средства разработки. IaaS – это самый низкий уровень, он подразумевает предоставление заказчикам виртуализированных инфраструктурных компонентов – серверных вычислительных ресурсов, систем хранения данных, сетевой инфраструктуры.

Несмотря на некоторые преимущества облачных вычислений, также присутствует риск потери или утечки данных. Использование облачных сервисов требует беспрецедентно высокого уровня доверия к сервис-провайдеру. Однако риски кражи данных не ограничиваются несанкционированными действиями со стороны провайдера или лиц предпринимающих атаку на сервис-провайдера. Велика вероятность того, что данные будут перехвачены во время обмена между пользователями и облачным сервисом интернет - провайдерами или сторонними злоумышленниками.

Для обеспечения безопасности необходимо использовать шифрование. Если в случае SaaS-модели или PaaS-модели, предоставляющей стек решений обеспечить безопасность сравнительно несложно (достаточно использовать SSL шифрование конкретного соединения), то в случае IaaS-модели, предоставляющей вычислительную платформу или IaaS-модели, в случае, когда необходима тесная интеграция с физической сетью предприятия, необходимо использовать VPN. VPN — частная сеть, работающая как туннель внутри сети большего масштаба и, таким образом, доступная только для определенных клиентских компьютеров. Однако существует множество различных технологий VPN и технологий реализации провайдерских сетей. Применение любой из VPN технологий неизбежно скажется на производительности соединения. Поэтому перед пользователями и поставщиками встаёт задача построения производительного, защищённого и лёгкого в обслуживании и настройке VPN соединения.

Данная работа посвящена выбору оптимального VPN соединения в современных провайдерских сетях.

Одной из популярных и наиболее перспективных технологий сетей провайдеров является технология MPLS. MPLS – механизм в сетях высокопроизводительных телекоммуникаций, который направляет и передает данные от одного узла сети к другому. MPLS работает на канальном уровне, который реализуется над канальным уровнем физического или логического соединения. На базе данной технологии провайдерами могут реализовываться VPN сети MPLS VPN и VPLS. К преимуществам данных технологий можно отнести масштабируемость, возможность пересечения адресных пространств, узлов подключенных в различные VPN, изолирование трафика VPN друг от друга на втором уровне модели OSI, а также возможность создания прозрачных соединений. Однако при работе с данной VPN необходимо учитывать, что она не обеспечивает целостности и конфиденциальности (шифрования) информации.

В работе рассмотрены и описаны основные технологии реализации VPN. Также выполнена оценка их производительности при работе поверх MPLS VPN и VPLS сетей. Для выполнения оценки производительности была симулирована работа MPLS сети. Критериями оценки являлись: время отклика и пропускная способность соединения. Помимо численных оценок в работе описаны конкретные проблемы, возникающие при настройке того или иного VPN соединения.

В результате работы представлены рекомендации по выбору оптимального VPN соединения в современных провайдерских сетях. Обозначены потенциальные проблемы MPLS сетей и предложены методы их решения.

Результаты данной работы могут быть применены сервис - провайдерами и пользователями PaaS и IaaS сервисов, а также интернет – провайдерами и компаниями, использующими технологию MPLS.

## **Информационно-образовательный портал по правовым аспектам защиты информации «LIS-Russia.NET»**

**Авторы: Бедиров Мурад Рамазанович**

**Пацукова Валентина Сергеевна, Чичиков Анатолий Александрович**

**Пятигорский государственный лингвистический университет  
Пятигорск, Россия**

Аннотация: Веб-ресурс, освещающий нюансы и являющийся навигатором по законодательству Российской Федерации в области защиты информации. В ближайшее время планируется в помощь иностранным компаниям и частным лицам, находящимся на территории РФ, полный перевод ресурса на английский язык.

Основной целью ресурса являлось создать систему, позволяющую человеку, будучи дилетантом в юридических науках, получить доступную справку по различным (бытовым, коммерческим, государственным) вопросам защиты информации. Говоря простым языком, лицо, задумав нарушение, может зайти на LIS-Russia.NET и увидеть, сколько за данное нарушение «светит». Компании, либо частные лица, заинтересованные в правовой защите своих продуктов, могут опубликовать ссылку на интересующий объект LIS-Russia.NET, например, рядом с кнопкой «принять лицензионное соглашение». Таким образом, появляется шанс, что злоумышленник одумается, увидев в подробностях масштабы наказания.

Для профессиональных юристов и людей, интересующихся законодательством, имеется подборка нормативно-правовых документов в области информации, информационных технологий и защиты информации с удобной системой навигации.

Актуальность проблемы киберпреступности в современном мире приняла, бесспорно, глобальные масштабы. Достаточно просмотреть отчеты аналитических служб о совершенных киберпреступлениях. Безусловно, информационная система не остановит «профессиональных» преступников, но совесть законопослушного гражданина сможет подсказать правильный выбор. А ведь если благодаря «LIS-Russia.NET» уровень киберпреступности снизится хоть на 0,5%, то его существование, несомненно, будет оправдано.

## **Data and education portal of legal issues in information security «LIS-Russia.NET»**

**Authors: Anatoly Chichikov, Murad Bedirov, Valentina Patsukova**

**Pyatigorsk State Linguistic University**

Annotation: This website was designed in order to be a navigator in the field of legal information security in Russia. In the nearest future we are planning to translate the whole site into English to make it possible for a foreign private person or an organization located in the Russian Federation to use it.

The main objective of this resource is to create a system which would provide an amateur in the science of law with available information referred to personal, commercial and national information security. To put it simply, once somebody has intended to commit a breach he can visit the site and see what punishment he will get. A company or a private person who wants to legally protect his software products can link them to an appropriate normative document of LIS-Russia.NET, for example one can build up a link next to "accept the license agreement" button. Realizing the potential level of punishment raises the chances of an intruder to make up his mind.

For professional lawyers and people who are interested in legislation the site includes a number of normative documents in the field of information, information technologies and information security along with a comfortable navigation system.

The cybercrime problem has undoubtedly become a global problem, which can be proved from the records of analytical departments from all over the world. Sure enough, the site will not stop professional criminals. Nevertheless we hope that it will help a law obedient person to make the right choice. And if it will and the cybercrime level will be decreased by at least 0,5% the creation of the site certainly will be proved to be reasonable.

## **Система обнаружения неизвестных вредоносных программ в корпоративной сети по анализу подозрительных действий**

**Авторы: Бердник Владимир Александрович, Цветков Максим Витальевич**

**Костанайский государственный университет имени Ахмета Байтурсынова, Факультет информационных технологий.  
Костанай, Республика Казахстан**

## **System on detection unknown malware in the corporate network via suspicious activities analysis.**

**Berdnik, Vladimir Alexandrovich; Tsvetkov, Maxim Vitalievich**

**Kostanai Akhmet Baitursynov State University, Faculty of Information Technologies.  
Kostanai, Republic of Kazakhstan.**

**Every “Cloud” dreams about our “Silver Lining”...**

In the given article the following issues are described the present situation in the issues of detecting malware; problems; strong and weak points of the methods used by malware to penetrate into PC.

On the basis of the analysis of these issues the strategy of detecting of unknown malware was formulated and the set to detect new malware on the basis of the analysis of suspicious software was developed. This set also provides comfortable administrating of found suspicious objects in the server part of the system.

This system was named **KSU Silver Lining (Kostanai State University)**.

**Every “Cloud” dreams about our “Silver Lining”...**

В настоящее время остро встал вопрос обеспечения антивирусной безопасности предприятий. Помимо общего высокого уровня вирусной активности, нарастает тренд развития целевых атак, характеризующихся наличием у организаторов подобных атак высококвалифицированных разработчиков, высокой «проникающей» способностью подобного вредоносного кода и потенциально – очень высоким ущербом для атакуемой организации.

В арсенале антивирусных компаний имеются хорошие методы борьбы с вредоносным ПО, такие как сигнатурный, эвристический, а также «облачные» технологии. Но, к сожалению, в современных условиях, их применения не всегда достаточно для своевременного обнаружения нежелательного кода, по целому ряду причин, описанных в нашей работе.

К тому же, администратор системы антивирусной безопасности предприятия, в настоящее время, не имеет технической возможности своевременно реагировать на появление в корпоративной сети неизвестного (нового) вредоносного программного обеспечения.

Мы, в рамках данной работы, поставили перед собой цель исследовать возможности улучшения ситуации и, на основе данных исследований, разработать программный комплекс, способный обнаруживать неизвестное вредоносное программное обеспечение по анализу подозрительных действий, выполняемых на локальном компьютере.

Результатом нашей работы явился достаточно удобный инструмент работы администратора сети предприятия, позволяющий выявлять неизвестное вредоносное программное обеспечение. Сейчас это является очень важным, поскольку количество ежедневно обнаруживаемых новых вредоносных программ преодолело отметку в 30 000 экземпляров, а возможность обнаружения вредоносного кода антивирусным программным обеспечением напрямую зависит от скорости попадания вредоносного объекта в антивирусную лабораторию (кроме методов эвристического анализа и «облачных» технологий). Данная система, получившая название **KSU Silver Lining (Kostanai State University)**, при условии внедрения ее в сети организации, позволит заметно сократить время обнаружения неизвестного кода, имеющегося на компьютерах предприятия. В ходе тестирования программа успешно обнаружила следующие образцы вредоносного кода (образцы были взяты учитывая распространенность в сети университета и демонстрации разных подходов в заражении, вредоносные объекты с аналогичными алгоритмами распространения также будут успешно обнаружены): **Trojan.Win32.Buzus.dfew**, **P2P-Worm.Win32.Palevo.bixy**, **Trojan.Win32.Pincav.alrv**, **Trojan.Win32.Scar.ddjd**, **Worm.Win32.Stuxnet.m**, **Virus.Win32.Virut.ce**, что доказало эффективность разработанной системы для решения задач обнаружения нового (неизвестного) вредоносного ПО (данные образцы были выявлены исключительно по поведению, без использования баз, поэтому их можно считать новым кодом для нашей системы).

Также данный подход может оказаться полезным в режимных учреждениях, где использование сети Интернет запрещено регламентами, а, следовательно, невозможно применение «облачных» технологий. Учитывая растущее число целевых атак на данные предприятий, предлагаемая система может существенно помочь в решении проблемы целевых вредоносных программ, разрабатываемых в единичных экземплярах и распространяемых без создания эпидемий, что сильно увеличивает время попадания вредоносного кода для анализа в антивирусную компанию.

По нашему мнению, предложенный подход можно было бы с успехом внедрить в систему централизованного управления антивирусной защитой предприятий, такую, как например **Kaspersky Administration Kit**. В этом случае будут достигнуты следующие цели: администраторы получат удобный инструмент обнаружения неизвестного вредоносного ПО, а также, будет решена проблема возможных конфликтов защитных средств (они будут в случае одновременного применения предлагаемого продукта и антивируса на одной машине) и существенно сокращены издержки вычислительных мощностей (не будет «торможения»), благодаря единой точке обработки подозрительного кода – в антивирусном продукте.

Если будет реализован подобный подход, по нашему мнению, появится реальная возможность продвинуться намного дальше в вопросах обнаружения неизвестного вредоносного ПО в целом и специфических, «целевых» вредоносных программ, в частности (в том числе и уязвимостей «нулевого дня»), а также проблемы таких типов вредоносных программ, как **Droppers** и **Downloaders**, которые иногда удаляются из системы после установки в нее вредоносного объекта с целью сокрытия путей его распространения), как одного из наиболее вероятных и опасных трендов развития вредоносного программного обеспечения.

## Повышение эффективности противодействия сетевым угрозам посредством интеграции технологий

Дугин Андрей Олегович

Украинский Научно-Исследовательский Институт Связи  
Украина

Due to continuous world-wide computerization network technologies progress process is very fast and information technologies are entering in any branch of modern business. Attack opportunities on these technologies are very wide too and there are several methods for attacks detection and prevention are developing. Every method has its' benefits and information technologies integration gives and ability to accumulate these methods together.

В условиях непрекращающейся компьютеризации сетевые технологии развиваются и проникают практически во все сферы современного бизнеса. Вместе с технологиями растут возможности взлома, проникновения, выведения серверов и сервисов из строя и прочих видов деструктивной активности. Наряду с этим развиваются методы защиты от вторжений и технологии противодействия атакам. Каждый набор методик имеет свои преимущества, которые можно суммировать при интеграции соответствующих систем.

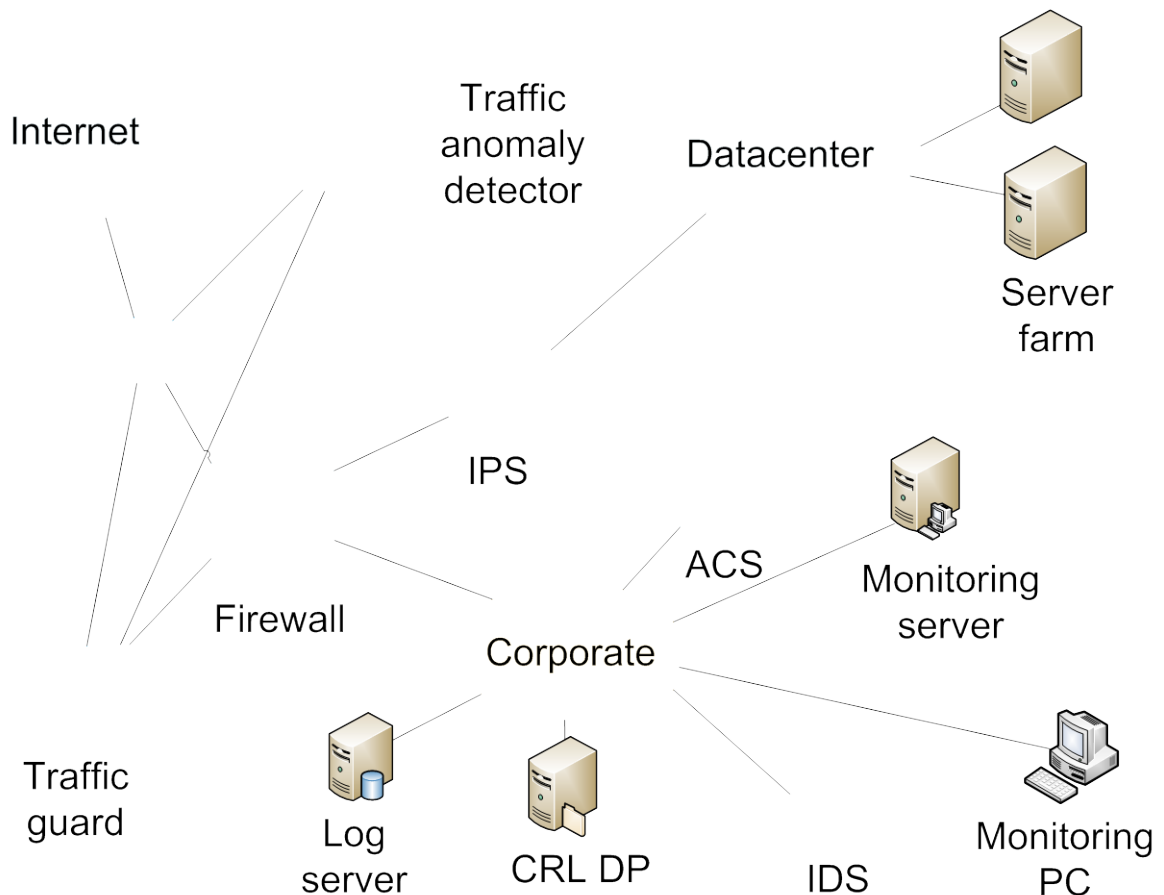
Сетевые угрозы можно условно разделить на активные и пассивные. Активные – угрозы, с помощью которых возможно воздействие на атакуемую систему, пассивные – направленные на изучение либо перехват передаваемых данных. Классификация атак по модели OSI указывает угрозы, соответствующие определенному уровню модели взаимодействия открытых систем. Для обеспечения сетевой безопасности также необходима безопасная настройка операционной системы, базы данных и сетевого приложения.

Проанализировав возможные атаки на всех семи уровнях модели OSI, несложно определить наиболее часто встречающиеся технологии и методики определения и минимизации угроз:

- - мониторинг устройств и сервисов;
- - межсетевые экраны;
- - системы обнаружения и предотвращения вторжений;
- - анализ лог-записей;
- - аудит безопасности.

Соответственно, правильным образом скомбинированный подход к комплексному использованию технологий безопасности и мониторинга дает возможность повышения уровня защищенности корпоративной инфраструктуры. Приведенная ниже схема инфраструктурного фрагмента позволяет объединить следующие преимущества использования перечисленных технологий:

- - оперативное реагирование на изменения;
- - маршрутизация, фильтрация и инспектирование трафика между подсетями;
- - VPN;
- - AAA;
- - NAT;
- - анализ сетевого трафика;
- - динамическое создание запрещающих правил на межсетевом экране на время атаки;
- - перенаправление вредоносного трафика на систему очистки – защита от DDoS;
- - корреляция лог-записей и событий систем обнаружения вторжений.



Если тема мониторинга статистических параметров сетевого и серверного оборудования раскрыта достаточно широко, то использование подобных результатов анализа для сетевых сенсоров систем обнаружения и предотвращения вторжений описано достаточно скудно. Одной из задач диссертации было исследование возможности использования статистических параметров IDS как вспомогательных в работе. Исследование проводилось в течение двух лет на инфраструктуре с использованием 20 сетевых сенсоров систем обнаружения вторжений двух разных производителей. Результаты и их практическое применение описаны в статьях [1-7] тематических журналов.

## Литература

1. Дугин А.О. Мониторинг Cisco IDS/IPS на примере модуля IDSM2 с помощью MRTG // Системный администратор, №5(78) май 2009. – с. 22-24.
2. Дугин А.О. Мониторинг Cisco IDS/IPS на примере модуля IDSM2 с помощью MRTG. Часть 2 // Системный администратор, №6(79) июнь 2009. – с. 38-39.
3. Дугин А.О. Cisco IDS/IPS. Безопасная настройка // Системный администратор, №8(81) август 2009.
4. Дугин А.О. Linux и системы обнаружения вторжений // Защита информации. Инсайд. №3, 2010. – с. 56-60.
5. Дугин А.О. Управление инфраструктурой систем обнаружения вторжений // Защита информации. Инсайд. №4, 2010.
6. Дугин А. О. Интеграция Cisco IDS/IPS и IBM ISS SiteProtector с OpenNMS // Системный администратор. № 5, 2010, с. 54–56.
7. Дугин А.О. Практические аспекты управления инфраструктурой IDS/IPS // "Information security/Информационная безопасность" №5, 2010 – с. 50-51.  
<http://itsec.ru/articles2/control/prakticheskie-aspekti-ypravleniya-infrastryktyroi-ids-ips>

## Оценка количества людей, имеющих персональные данные в открытом доступе (на примере города Магнитогорска)

Калиновский Евгений Александрович  
Магнитогорский государственный университет

## Estimation of quantity of people who have open access to the information privacy (for example Magnitogorsk)

Kalinovsky Eugene Alexandrovich  
Magnitogorsk State University

### Annotation

The central purpose of the research is the try to determine the quantity of people of the city who have open access to the information privacy, thereby running the risk of illegally using these data. The researches were conducted on basis of the analysis of the text information in internet. Scope of the inquiry is limited to inhabitants of Magnitogorsk.

### Аннотация

Основной целью исследования является попытка определить количество жителей города, имеющих персональные данные в открытом доступе и таким образом подвергающихся риску неправомерного использования этих данных. Исследование проводилось на основе анализа текстовой информации сети Интернет. Область исследования ограничена жителями г. Магнитогорска.

Данное исследование было направлено на попытку проанализировать степень конфиденциальности информации о людях, имеющих свои персональные данные в сети Интернет (в открытом доступе), а так же установить источники, в которых можно найти наибольшее количество персональных данных.

### Цели и задачи работы

Определить количество людей, имеющих персональные данные в Интернете.

Указать основные источники персональных данных. Исследовать источники на достоверность информации.

Выделить группы людей, и указать процент распределения их персональных данных в Интернете.

Указать и исследовать особенности источников, повышающие информативность персональных данных. Указать возможные риски безопасности людей, имеющие свои персональные данные в Интернете.

Актуальность исследования подкреплена Федеральным законом Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных.

В ходе исследования было установлено, что наибольший объем персональных данных жителей города содержится в социальных сетях. Доля жителей города, имеющих персональные данные в открытом доступе и подвергающих себя различным рискам, составляет примерно 25%. Большая часть персональных данных выкладывается самими жителями.

Вопрос о практическом применении полученных результатов в сфере информационной безопасности обозначился в ходе исследования. Как выяснилось, более всего различным рискам подвержены пользователи социальных сетей. Вопрос о безопасности в социальных сетях требует дальнейшего детального исследования. Так же, были получены результаты о размещении персональных данных в открытых источниках. Оказалось, что в таких источниках содержится четверть населения города Магнитогорска.

## Автоматическое детектирование новых вредоносных программ на базе структурной информации о PE-файле

Кипер Андрей Борисович  
Ляшенко Елизавета Владимировна

Одесский Национальный Политехнический Университет  
Одесса, Украина

Основные используемые методы детектирования вредоносного ПО обеспечивают высокую эффективность детектирования уже известных экземпляров вредоносных файлов, но показывают плохие результаты при детектировании ранее неизвестных файлов. В работе представлен подход к детектированию новых вредоносных программ, дающий вердикт, основанный на структурных данных исполняемого файла PE-формата с использованием технологий извлечения знаний.

В рамках работы была создана система, состоящая из 3-х модулей: (1) PE-Parser, (2) Data Mining Tool, (3) Malware Classifier. PE-Parser извлекал необходимую структурную информацию из файла (DOS-заголовок, NT-заголовок, таблицу секций), Data Mining Tool использует данные, полученные из первого модуля и обучает систему и Malware Classifier совершает классификацию подаваемого на вход файла из двух классов (безопасное ПО, вредоносное ПО). В качестве используемого алгоритма обучения и классификации был использован алгоритм деревьев решений C4.5.

В работе была произведена опытная проверка системы на подборке, состоящей из 83291 файла, разделенной на 2 части: обучающая выборка (31202 файла, 11644 безопасных и 19558 вредоносных) и тестовая выборка (52089 файлов, 10630 безопасных и 41459 вредоносных). Получены следующие результаты:

1. Точность детектирования по обучающей выборке: 99.4%
2. Точность детектирования по тестовой выборке: 90.9%
3. Точность детектирования безопасных файлов: 87.3%
4. Точность детектирование вредоносных файлов: 96.6%
5. Общая точность системы: 94.1%

Также было произведено тестирование устойчивости подхода к изменениям в структуре исполняемых файлов с использованием нескольких популярных упаковщиков. Тестирование показало, что использование известных (участвовавших в обучении) способов преобразования файла не влияет на качество детектирования, в то время как использование ранее неизвестного способа преобразования файла способно обмануть систему.

В завершение, были проанализированы достоинства и недостатки подхода, и было установлено, что предложенное решение можно использовать в сочетании с другими методами детектирования, а также для выдачи предварительного вердикта по файлу.

## Анализ стратегий защиты цифровых программных продуктов от интернет-пиратства с использованием метода экономико-математического моделирования

Автор Лаушкин Алексей Николаевич

Донецкий национальный университет  
Донецк, Украина

## ANALYSIS OF PROTECTION STRATEGIES OF DIGITAL SOFTWARE PRODUCTS AGAINST INTERNET PIRACY WITH THE USE OF ECONOMETRIC MODELLING METHODS

Author Laushkin Oleksii Mykolayovich

Donetsk national university  
Donetsk, Ukraine

**Summary.** In the article, the author, with the use of an econometric apparatus, analyzed comparative efficiency of micro- and macroeconomic instruments in diminishing the scopes of Internet piracy in the sphere of downloadable software. As the result of the scientific research, low influential efficiency of macroinstruments on consumers' behavior was revealed. Reliability and practical significance of the results was confirmed with regard to protection policy for ZAO "Kaspersky Lab" digital products.

**Аннотация.** В статье автор, с использованием экономико-математического аппарата, проанализировал сравнительную эффективность микро- и макроэкономических инструментов в сокращении масштабов Интернет-пиратства в сфере загружаемого программного обеспечения. В результате проведенного исследования, была выявлена низкая эффективность макроинструментов влияния на потребительское поведение. Достоверность и практическая значимость полученных в результате моделирования выводов была подтверждена применительно к практике защиты программных продуктов ЗАО «Лаборатория Касперского».

**Цель исследования.** Целью данной работы является выработка действенных микро- и макроинструментов сокращения масштабов пиратства на монополизированных рынках загружаемого программного обеспечения.

**Задачи исследования.** В качестве первостепенных, были выделены следующие задачи:

- проанализировать современное состояние рынка цифрового загружаемого ПО и выявить проблемы, препятствующие его эффективному функционированию;
- разработать экономико-математическую модель для сравнительного анализа эффективности мер сдерживания роста масштабов рынка загружаемого пиратского ПО;
- выработать предложения по совершенствованию политики ЗАО «Лаборатория Касперского» в сфере противодействия нелегальному использованию объектов интеллектуальной собственности – программных решений для обеспечения информационной безопасности.

**Актуальность.** В конце XX в., информационные продукты, записанные на физические носители (дискеты, CD, DVD диски), реализовывались через традиционные каналы сбыта. Информационные технологии XXI в., с одной стороны, открыли новые возможности продвижения данных продуктов через цифровые сети, а с другой – положили начало процессу становления рынка нелегального загружаемого ПО.

С момента опубликования первых статистических данных о масштабах и прямых экономических потерях от пиратства в сфере программного обеспечения, правительства многих стран и международные организации стали проводить регулярный мониторинг развития данной проблемы. Так, согласно информации Business Software Alliance, в 2009 г. доля пиратского программного контента в совокупном объеме установленного на персональных компьютерах ПО увеличилась на 2% в сравнении с предыдущим годом и достигла 43%. Для сравнения, в Украине данный показатель в 2009 г. достиг отметки в 85% (83% в 2007 г.), а прямые экономические потери были оценены в 272 млн. долл. США. Теоретические и эмпирические исследования

глобального рынка нелегального загружаемого ПО, свидетельствуют о наличии тесной корреляционной связи между уровнем цифрового пиратства в стране и долей вредоносного ПО, которое установлено на пользовательских компьютерах.

Рост значимости феномена пиратства в сфере цифрового программного обеспечения в условиях интеграции экономик многих стран, дал начало исследованиям, ставящим своей целью изучение поведенческих, этических и экономических особенностей функционирования специфического рынка нелегального цифрового загружаемого контента.

Основные результаты исследования. В результате проведенного анализа экономико-математической модели рынка цифрового программного обеспечения, приходим к следующим выводам:

- В случае превышения значения экстерналий сетевых эффектов над величиной полных ожидаемых издержек от пиратства, объем реализации нелегального цифрового контента снижается с ростом издержек на его получение.
- Рост воспринимаемой потребителем вероятности понести наказание за незаконные действия, связанные с нарушением прав интеллектуальной собственности, приводит не к сокращению, а к увеличению объема реализации нелегального цифрового контента.
- Изменение величины штрафа за нарушение прав законных владельцев информационного продукта не оказывает влияния на уровень Интернет-пиратства в сфере программного обеспечения.

В результате анализа полученных выводов проявились первопричины низкой эффективности осуществляемого макрорегулирования рынка нелегального цифрового ПО. Превентивные меры, основанные на директивном регулировании степени материальной ответственности нарушителя прав интеллектуальной собственности, не только не ведут к сокращению общего количества пользователей нелегального цифрового контента, а и стимулируют его дальнейший рост. По нашему мнению, решение данного парадокса может быть найдено на микроуровне потребительских предпочтений и воспринимаемой полезности товара.

Увеличение издержек на получение пиратского ПО, в частности, времени на поиск, разблокировку, защиту от вирусных атак и, в случае его неработоспособности, поиск работоспособных аналогов, могут значительно снизить потребительскую полезность нелегального программного контента. Вместе с тем, дополнительное постпродажное обслуживание, низкая стоимость обновления до более новых версий, развитие версифицирование и бесплатные тестовые периоды позволят обеспечить стабильный платежеспособный спрос на официальный цифровой продукт.

Таким образом, именно на микроэкономическом уровне должны быть реализованы ключевые мероприятия:

- инвестирование в инновационные разработки, реализация крупных IT-проектов путем межфирменной кооперации, что позволит производить качественный цифровой продукт по ценам ниже издержек на получение пиратского аналога;
- создание мощных сбытовых каналов в сети Интернет;
- разработка информационных продуктов, способных адаптироваться к индивидуальным потребностям пользователей, что позволит перейти от монопольной к конкурентной рыночной организации, одновременно снизив массовый спрос на нелегальные копии основных программных продуктов фирмы-монополиста.
- обеспечение индексирования сайтов, продвигающих лицензионный продукт в ведущих поисковых системах (Google, Yahoo, MSN и др.), что сведет к минимуму вероятность для потребителя в первых строках результатов поиска встретить ссылки на бесплатное скачивание пиратского цифрового контента;
- проведение кампаний, ставящих своей целью не создание негативного образа пользователя пиратской программной продукции, а доведение до сведения потенциальных потребителей выгод от использования лицензионного ПО.

Практическое применение в сфере информационной безопасности. Применительно к продуктам ЗАО «Лаборатория Касперского», которые подвержены влиянию весьма специфического вида пиратства – нелегального распространения ключей активации лицензии, стандартные ограничительные механизмы их защиты зачастую проявляют свою низкую эффективность. В данном случае, основываясь на выводах разработанной экономико-математической модели, а именно на положении 1, рост количества пользователей продуктов ЗАО «Лаборатория Касперского» (пользующихся программами, активированными с помощью лицензионных и пиратских ключей) приведет к интенсификации внешних сетевых эффектов, что, в конечном счете, стимулирует потребителей перейти на лицензионный цифровой продукт. Тем не менее, уровень пиратства, который максимизирует прибыль, должен быть регулируемым и контролируемым самой компанией. В противном случае, неконтролируемое копирование официальных продуктов

ведущего игрока рынка антивирусного ПО нанесет ущерб репутации и отразится на финансовом положении фирмы.

Эффективность существующей практики блокирования ключей активации продуктов ЗАО «Лаборатория Касперского», регулярно публикуемых в сети Интернет, и внесения их в так называемый «черный список» при обновлении, подтверждается результатами моделирования. Рост транзакционных издержек поиска и установки «рабочих» (не заблокированных) ключей снижают полезность пиратских антивирусных программ компании для пользователя. Игнорирование необходимости систематического обновления, что позволяет ПО функционировать с пиратским ключом активации, помимо неудобств из-за периодического напоминания антивирусным продуктом об устаревших вирусных базах, представляет значительную угрозу безопасности ПК потребителя. Обобщая вышесказанное, необходимо отметить, что разработанная экономико-математическая модель рынка цифрового загружаемого ПО, теоретически подтверждает эффективность политики ЗАО «Лаборатория Касперского» в сфере противодействия нелегальному использованию объектов интеллектуальной собственности – программных решений для обеспечения информационной безопасности для конечных пользователей.

Эффективная политика взаимодействия производителя и потенциального потребителя цифровых программных продуктов должна дополняться пересмотром роли инструментов макрорегулирования данного рынка. Постепенный переход функции государства в данном вопросе от наказания недобросовестных пользователей к созданию предпосылок для улучшения бизнес-климата и повышения общественного благосостояния, позволит решить проблему пиратства в сфере загружаемого программного обеспечения без применения жестких директивных процедур.

## **Детектирование вредоносных соединений методом нейронных карт Кохонена**

**Миникаев Ришат Фаритович**

**Московский Физико-Технический Институт (Государственный Университет)  
Москва, Россия**

В работе проведено исследование алгоритма самоорганизующихся карт Кохонена и возможность его применения в информационной безопасности. На основе данного алгоритма была создана программа, осуществляющая анализ сетевой активности и определяющая вредоносные соединения.

## **Detection of malicious connections by Kohonen Self Organizing Maps**

**Minikaev Rishat Faritovich**

**Moscow Institute of Physics and Technology**

In the work is analyzed algorithm of Kohonen Self Organizing Maps and their availability in information security. On the basis of this algorithm was created program carries out an analysis of network activity and determining the malicious connections

В настоящее время существует огромное количество вредоносных программ распространяющихся в самых разнообразных системах и сетях передачи данных. Для детектирования этих программ существует множество методов и способов, но со стремительным развитием Интернета количество вредоносных программ увеличивается, а адекватная скорость их детектирования. Одним из методов, позволяющих ускорить и облегчить детектирование угроз являются методы и алгоритмы на основе искусственного интеллекта. К таким алгоритмам искусственного интеллекта можно причислить алгоритм на основе самоорганизующиеся карты Кохонена. Цель исследования заключалась в изучении работы и применения алгоритма самоорганизующихся карт Кохонена к информационной безопасности.

Самоорганизующаяся карта (СОК) является новым и эффективным программным инструментом для визуализации многомерных данных. В своём основном варианте СОК создаёт граф подобия входных данных. Она преобразует нелинейные статистические соотношения между многомерными данными в простые геометрические связи между изображающими их точками на устройстве отображения низкой размерности, обычно в виде регулярной двумерной сетки узлов. Поскольку СОК осуществляет сжатие информации с сохранением в получаемом изображении наиболее важных топологических и метрических связей между первичными элементами данных, можно также считать, что с её помощью порождаются обобщения некоторого вида. Эти два характерных свойства СОК, визуализацию и обобщение, можно использовать различными способами в решении сложных задач таких, как анализ процессов, машинное восприятие, управление, передача информации. В той форме, в которой она существует в настоящее время, СОК была задумана Т. Кохоненом в 1982 г.

Изначально, самоорганизующаяся карта представляет собой гексагональную сетку из узлов, соединённых между собой связями. Также определяется количество нейронов в сети.

Каждый из узлов описывается двумя векторами. Первый — вектор веса  $m_i$ , имеющий такую же размерность, что и входные данные. Второй — координаты узла на карте, вектор  $r_i$ . Перед началом обучения карты необходимо проинициализировать весовые коэффициенты нейронов.

На каждом шаге обучения из исходного набора данных случайно выбирается один из векторов

$x = \{\xi_1, \xi_2, \dots, \xi_n\}^T \in R^n$ , где  $n \in N$ , а затем производится поиск наиболее похожего на него вектора коэффициентов нейронов. При этом выбирается нейрон-победитель, который наиболее похож на вектор входов, иными словами, определяется расстояние между векторами, которое обычно вычисляется в евклидовом пространстве. Если обозначим нейрон-победитель символом  $c$ , то получим:  $\|x - m_c\| = \min\{\|x - m_i\|\}$  или  $c = \arg \min\{d(x, m_i)\}$ , т.е.  $c$  - номер элемента, для которого расстояние до  $x$  минимально.

В случае, если таких победителей больше одного, то случайным образом выбирается единственный нейрон-победитель.

После того, как найден нейрон-победитель, производится корректировка весов нейросети. При этом вектор, описывающий нейрон-победитель, и векторы, описывающие его соседей в сетке, перемещаются в направлении входного вектора по формуле:

$$m_i(t+1) = m_i(t) + h_{ci}(t)[x(t) - m_i(t)], \text{ где } h_{ci}(t) - \text{ функция соседства.}$$

Циклический процесс обучения, перебирающий входные данные, заканчивается по достижении картой допустимой (заранее заданной аналитиком) погрешности, или по совершении заданного количества итераций. Вычисление ошибки карты рассчитано как среднее арифметическое расстояний между наблюдениями и векторами весов соответствующего им нейрона – победителя:

$$\frac{1}{N} \sum_{i=1}^N \|x_i - m_c\|, \text{ где } N - \text{ количество элементов набора входных данных.}$$

Для визуализации структуры кластеров, полученных в результате обучения карты, применяется унифицированная матрица расстояний (u-matrix). Элементы матрицы определяют расстояние между весовыми коэффициентами каждого нейрона и его ближайшими соседями. Затем эти значения используются для определения цвета, которым узел будет отрисован. При таком использовании узлам с большим расстоянием между ними и соседями соответствует чёрный цвет, а близлежащим узлам – белый.

На основе алгоритма самоорганизующихся карт Кохонена была создана программа, реализующая этот алгоритм для определения вредоносных сетевых соединений, выполненных программными закладками. Входными данными, используемыми программой является 9-тимерный входной вектор из IP адреса получателя, обратная зона DNS IP адреса получателя, электронная почта из WHOIS записи. Использовалась гексагональная сетка 7x5. В результате обработки программой входных данных, отрисовывается визуальная картина сетевой активности, а также производится кластеризация сетевых соединений методом кластеризации k-means. Было выделено три кластера, в каждый из которых 9-ти мерные вектора помещались на основе предположения о том, что соединения является, может являться или не является вредоносным.

Благодаря результатам работы этой программы можно получить данные о сетевой активности той или иной программы, а также определить является ли эта активность опасной, подозрительной или не представляющей опасность.

#### ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Кохонен Т. Самоорганизующиеся карты – М.: БИНОМ, Лаборатория знаний, 2008. – 655 с.
2. Зиновьев А.Ю. Визуализация многомерных данных. – Красноярск: Изд. Красноярского гос. технич. ун-та, 2000. – 180 с.

## ИНФРАСТРУКТУРА ДИАГНОСТИРОВАНИЯ СПАМА В ИНДИВИДУАЛЬНОМ КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

Мищенко А.С., Хаханова Ю.В.

Проф., д.т.н. Хаханов В.И., проф., д.т.н. Чумаченко С.В.  
Харьковский национальный университет радиозлектроники,  
Харьков, Украина

Актуальность данного исследования обусловлена тем, что кибернетическое пространство подвержено влиянию деструктивных компонентов, влияющих на работоспособность субъектов, которыми являются компьютеры, системы и сети. Поэтому сейчас и в будущем важной проблемой остается стандартизация пространства и специализация всех взаимодействующих субъектов, включая негативные, как неотъемлемую часть экосистемы. Среди модулей такой экосистемы можно выделить обнаружение спама путем анализа информации.

Целью данной работы является существенное повышение качества индивидуального кибернетического пространства (ИКП) пользователя и уменьшение стоимости эксплуатационных расходов за счет вакцинации ИКП путем добавления в пространство инфраструктуры сервисного обслуживания, включающей библиотеки позитивных и негативных сообщений и обеспечивающей тестирование, диагностирование и устранение вредоносных компонентов электронных писем.

Объект исследования – индивидуальное кибернетическое пространство, представленное информацией, ее носителями и преобразователями, а также деструктивными компонентами, наносящими вред функциональностям, улучшающим качество жизни человека.

Предмет исследования – инфраструктура сервисного обслуживания, включающая библиотеки позитивных и негативных сообщений и встроенную программную избыточность, которая работает в реальном масштабе времени, обеспечивает тестирование, диагностирование и устранение вредоносной и «мусорной» информации электронных писем, описанных в соответствующих библиотеках.

На основании разработки плагина для почтового клиента SquirrelMail были получены практические результаты, позволяющие из всего множества писем, приходящих на почтовый ящик, «спам» (анонимные массовые рассылки), частично идентифицировать уже не как спам, а как рассылка, которая может нести интересную информацию для пользователя.

Научная новизна результатов исследования заключается в том, что впервые предложена инфраструктура сервисного обслуживания индивидуального кибернетического пространства, которая характеризуется наличием встроенных средств тестирования, диагностирования и восстановления ИКП и двух пополняемых библиотек позитивных и негативных сообщений, что дает возможность существенно (в несколько раз) уменьшить время анализа получаемой информации.

Практическая значимость результатов исследования инфраструктура сервисного обслуживания ИКП ориентирована на повышение качества жизни всех субъектов планеты, использующих почтовые сервисы для коммуникации с внешним миром. При этом ИКП – модель будущего общения человека с внешним миром, которая инвариантна по отношению к техническим средствам доступа в киберпространство планеты.

В качестве направления будущих научных исследований следует выделить проблему создания теории, методов и архитектуры параллельного анализа информации, представленной в виде аналитических, графовых и табличных форм ассоциативных отношений для поиска, распознавания, диагностирования деструктивных компонентов и принятия решений в n-мерном векторном дискретном пространстве.

Ожидаемые результаты и их рыночная привлекательность состоят в следующем: 1) Инфраструктура встроенной защиты программного кода от несанкционированной модификации, приводящей к изменению функциональности. 2) Избыточность инфраструктуры программного кода, которая автоматически синтезируется на стадии проектирования и верификации, составляет не более 5% от специфицированной функциональности. 3) Рыночная привлекательность

инфраструктуры, определяемая многообразием программных продуктов, умноженной на уровень продаж каждого изделия, составляет в год порядка одного миллиарда экземпляров. 4) Стоимость создания инфраструктуры для программного продукта составляет 20% затрат от разработки функционального кода. Если уровень продаж – не менее 500 копий, то затраты на создание встроенного антивируса вполне окупаемы в течение года. 5) Внедрение запатентованной технологии вакцинации программных продуктов при их рождении может принести компании порядка 2-х миллиардов долларов в первые 3 года ее эксплуатации. 6) Маркетинговая проблема глобальной компании (Лаборатория Касперского) заключается в убеждении разработчиков программных продуктов имплементировать существующие внешние антивирусы вовнутрь кода полезной функциональности.

## Особенности использования метода case-study при преподавании информационной безопасности

Савельева А.А.

Государственный Университет – Высшая Школа Экономики

*В данной работе предлагается подход к преподаванию информационной безопасности, основанный на использовании метода case study для проведения практических занятий. Обосновывается целесообразность применения метода case study на примере его использования в рамках курсов «Организация и технология защиты информации» и «Технологии обеспечения информационной безопасности», читаемых студентам магистратуры и бакалавриата отделения программной инженерии ГУ-ВШЭ с 2008 г. Данная работа восполняет отсутствие методических рекомендаций по использованию метода case study при преподавании в высших учебных заведениях дисциплин, связанных с защитой информации.*

**Ключевые слова:** информационная безопасность, case study, управление рисками, методические рекомендации

## Teaching Information Security: a Case-Study Approach

Alexandra A. Savelieva

State University – Higher School of Economics, Russia

*In this paper we propose a new approach to teaching practical information security in higher school based on case studies. We justify its place in information security curriculum by providing an example from our experience of using the approach for BSc and MSc students of Higher School of Economics in the courses on “Technical and Organizational Aspects of Information Security” and “Information Security Technologies”. This paper fills the gap in existing practices for teaching information security which currently lack in guidelines for designing case studies and integrating them into the curriculum.*

**Keywords:** Information security, case study, Risk management, best practices

Метод case study (кейс-стади, метод конкретных ситуаций) представляет собой интерактивную технологию для обучения на основе реальных или вымышленных бизнес-ситуаций, способствующую не только усвоению знаний, но и формированию у слушателей аналитических навыков и умений разрешения проблемных ситуаций. Словарь [Грицанов2003] описывает case study как «исследовательский проект, в котором в качестве предмета исследования выбирается единичный случай или несколько избранных примеров ... и определяется совокупность методов их изучения».

Метод конкретных ситуаций возник в начале XX в. в Школе бизнеса Гарвардского университета, известной своими инновациями [Зобов2006]. Распространение метода в мире началось в 70-80 годы, тогда же метод получил известность и в СССР. Анализ ситуаций начал использоваться при обучении управленцев, в основном на экономических специальностях ВУЗов, в первую очередь как метод обучения принятию решений. Значительный вклад в разработку и внедрение этого метода внесли Г.А. Брянский, Ю.Ю. Екатеринославский, О.В. Козлова, Ю.Д.Красовский, В.Я. Платов, Д.А. Поспелов, О.А. Овсянников, В.С. Рапопорт и др.

Создание учебной среды, способствующей развитию навыков анализа информации, обнаружения связей между фактами и формирования гипотез, было признано особенно актуальным после публикаций западными исследователями статей о несоответствии уровня образования потребностям современного общества (см. [Chipman1985, Brown1989, Nickerson1988, Resnick1987]).

Новая волна интереса к методу case study в России началась в 90-е годы в связи с ростом спроса на специалистов, умеющих действовать в ситуациях, связанных с риском или неопределённостью, анализировать проблемы и принимать обоснованные решения. Это привело к распространению практики использования метода case study в программах гуманитарных и экономических дисциплин, таких как политология, менеджмент, маркетинг, социология и т.д. (см., например, [Багиев2005, Камински1998, Парамонова2009, Грицанов2003]).

Одной из главных тенденций образования в области защиты информации является осознание необходимости использования принципов управления рисками при решении проблем, связанных с обеспечением информационной безопасности [Blakley2001, ISO2008]. Эта тенденция особенно ясно прослеживалась в условиях мирового финансового кризиса, т.к. с ростом количества «обиженных» в результате сокращений сотрудников увеличивалась вероятность совершения преступлений в отношении информационных ресурсов предприятий. Наиболее востребованными становятся специалисты по обеспечению информационной безопасности, умеющие учитывать не только на технические, но организационные аспекты обеспечения ИБ. Это делает целесообразным применение для подготовки специалистов по защите информации метода case study, показавшего свою эффективность для развития навыков анализа ситуаций и принятия решений в условиях реального мира. Однако, как показал анализ российских и англоязычных публикаций, до сих пор отсутствуют методические разработки по использованию метода case study при преподавании в высших учебных заведениях дисциплин, связанных с защитой информации.

В данной работе предлагается подход к преподаванию информационной безопасности, основанный на использовании метода case study для проведения практических занятий. Описывается методика разработки case study по информационной безопасности и приводятся примеры, используемые при чтении курсов «Организация и технология защиты информации» и «Технологии обеспечения информационной безопасности» студентам магистратуры и бакалавриата отделения программной инженерии ГУ-ВШЭ. В заключении приводятся выводы о влиянии метода case study на ход учебного процесса и освоение студентами материалов курса, сделанные на основе опыта применения данного подхода.

Преимуществами подхода к преподаванию информационной безопасности, основанного на использовании метода case study, являются:

- ориентация на практические аспекты обеспечения ИБ в условиях реального мира
- высокий уровень вовлеченности студентов
- фокусирование внимания студентов не только на технических, но и на организационных аспектах обеспечения ИБ
- демонстрация необходимости применения методов управления рисками для обеспечения защиты информации
- возможность проведения практических занятий при минимальном уровне оснащенности аудитории
- комплексный подход к проблеме обеспечения ИБ с разных позиций – пользователя, технического специалиста, финансового директора, архитектора и топ-менеджера

Предлагаемый подход внедрен в учебный процесс кафедры «Управление разработкой программно-обеспечения» отделения программной инженерии Государственного университета – Высшей школы экономики в рамках учебных курсов «Организация и технология защиты информации» (Магистратура; программа: Управление разработкой программного обеспечения"; 2-й курс, 1, 2 модуль) и «Технологии обеспечения информационной безопасности» (Бакалавриат; спец-я Программная инженерия"; 4-й курс, 3 модуль). Апробация подхода была проведена на конференции-марафоне Training Labs'2010 в формате интерактивного тренинга «Кейс-стади: управление рисками в мире цифровых зависимостей», разработанного на основе материалов курса «Организация и технологии защиты информации». Курс «Технологии и продукты Microsoft в

обеспечении информационной безопасности», в основу которого легло использование предлагаемого подхода, на конкурсной основе получил поддержку в виде гранта «Разработка курсов по информационным технологиям», организованного компанией Microsoft (курс опубликован в библиотеке учебных курсов Центра образовательных ресурсов Microsoft [Авдошин2010a] и в Интернет-Университете Информационных Технологий [Авдошин2010b], где имеет высокий рейтинг популярности – 4,83 из 5 по состоянию на 19.12.2010).

#### Использованная литература

1. [Зобов2006] Зобов А.М. Метод изучения ситуаций (case-study) в образовании: его история и применение // Центр дистанционного образования Elitarium, 2006. Интернет-ресурс: <http://www.elitarium.ru>
2. [Багиев2005] Багиев Г.Л. Руководство к практическим занятиям по маркетингу с использованием кейс-метода/ Г.Л. Багиев, В.Н. Наумов. – М., 2005.
3. [Камински1998] Камински Х. Дидактико-методические основы преподавания экономики. Изучение конкретного случая (case-study) // Экономика. Вопросы школьного экономического образования. – 1998. - №2.
4. [Парамонова2009] Парамонова Т.Н. Маркетинг: активные методы обучения / Т.Н. Парамонова, А.о. Блинов, Е.Н. Шереметьева, Г.В. Погодина. – М.: КНОРУС, 2009.
5. [Грицанов2003] Социология: Энциклопедия / Сост. А.А. Грицанов, В.Л. Абушенко, Г.М. Евелькин, Г.Н. Соколова, О.В. Терещенко., 2003 г
6. [Blakley2001] Bob Blakley, Ellen McDermott, Dan Geer. Information security is information risk management // NSPW '01 Proceedings of the 2001 workshop on New security paradigms, ACM, 2001
7. [Brown1989] Brown, J. S., Collins, A., & Duguid, P. (1989). Situated cognition and the culture of learning. Educational Researcher, 17, 32-42.
8. [Chipman1985] Chipman, S., Segal, J., & Glaser, R. (1985). Thinking and learning skills: Current research and open questions (Vol. 2). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.
9. [Jones1990] Jones, B. F., & Idol, L. (1990). Conclusions. In B. F. Jones & L. Idol (Eds.), Dimensions of thinking and cognitive instruction (pp. 511-532). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.
10. [Nickerson1988] Nickerson, R. S. (1988). On improving thinking through instruction. Review of Research in Education, 15, 3-57.
11. [Resnick1987] Resnick, L. B. (1987). Education and learning to think. Washington, DC: National Academy Press. Resnick, L. B., & Klopfer, L. E. (Eds.). (1989). Toward the thinking curriculum: Current cognitive research. Alexandria, VA: Association for Supervision and Curriculum Development.
12. [ISO2008] ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management.
13. [Авдошин2010a] Авдошин С.М., Савельева А.А., Сердюк В.А. «Технологии и продукты Microsoft в обеспечении информационной безопасности» // Библиотека учебных курсов Центра образовательных ресурсов Microsoft, 2010, <https://www.facultyresourcecenter.com/curriculum/pfv.aspx?ID=8476&Login=>
14. [Авдошин2010b] Авдошин С.М., Савельева А.А., Сердюк В.А. «Технологии и продукты Microsoft в обеспечении информационной безопасности» // Интернет-Университет Информационных Технологий, 2010, <http://www.intuit.ru/department/security/mssec/>

## **Международная защита интеллектуальной собственности в сфере компьютерных технологий**

**Титова Мария Александровна**

**International Copyright Protection in Computer Technology**

**Maria Titova**

**Московский Институт Экономики Менеджмента и Права (МИЭМП)  
Москва, Россия**

Во всем мире обозначилась тенденция перехода от сырьевой модели экономики – к инновационной.

Общемировая тенденция к обновлению законодательной базы по вопросам защиты интеллектуальной собственности, увеличению потоков экспорта и импорта программного обеспечения, усиления взаимointegrации экономик и роста доли международного аутсорсинга.

Необходимость совершенствования российского законодательства по вопросам защиты интеллектуальной собственности в сфере компьютерных технологий для интеграции в мировое экономическое сообщество с целью превращения РФ из «сырьевого придатка» в экспортера высоких технологий.

Российское законодательство по защите исключительных прав – его становление, анализ текущего положения и перспектив изменения, с учетом влияния развития компьютерных технологий на защиту данных и прав копирования.

Точки зрения ученых-исследователей о перспективах вступления России в ВТО и изменений законодательства по защите исключительных прав.

Ключевые международные конвенции по защите интеллектуальной собственности, анализ правового опыта ведущих экспортеров и импортеров программного обеспечения; рекомендации по совершенствованию российского законодательства.

Правовые вопросы экспорта компьютерных технологий и охраны исключительных прав; характеристика современной ситуации по экспорту высокотехнологичных продуктов и практические вопросы обеспечения этого процесса.

Исследование защиты исключительных прав в сфере компьютерных технологий в России и за рубежом, выявление проблем защиты российских программных разработок в иностранных государствах и анализ российских и общемировых правовых тенденций по защите интеллектуальной собственности в данной сфере, выявление путей решения названных проблем.

Необходимость активной маркетинговой политики России для зарубежных инвесторов, как государства надежного, открытого для инвестиций, гарантирующего защиту прав зарубежных инвесторов, предлагающего различные преференции и льготы.

Синдром «Оффшорного программирования».

С неизбежным вступлением России в ВТО, грядет изменение законодательства по защите интеллектуальной собственности в сфере компьютерных технологий. Данный фактор будет содействовать интеграции российских программных разработчиков и производителей программного обеспечения в мировую экономическую систему; обяжет к введению международных стандартов ведения бизнеса и обслуживания клиентов (таких как ISO9000 и CMM/CMMI). Это позволит улучшить Государства на мировой бизнес-арене и превратить Россию для зарубежных инвесторов из *tierra incognita* в среду, желанную для инвестирования. Облегчение интеграции произойдет за счет унификации базовых норм по защите интеллектуальной собственности для всех государств-членов Организации, а значит сократятся расходы и риски, например, при открытии представительства и пункта технической поддержки компьютерного продукта в другой стране.

Внимание законодательной регламентации правоотношений в сфере права интеллектуальной собственности на программное обеспечение.

Необходимость выделения программы для ЭВМ как самостоятельного объекта защиты, а не как литературного произведения. Это объясняется тем, что в отличие от написанного литературного произведения, написанную программу для ЭВМ нельзя прочитать. Текст компьютерной программы в большинстве случаев является закрытой информацией, не находящейся в свободном доступе.

Необходимость существенного ужесточения наказания за использование нелицензионного программного обеспечения.

Необходимость законодательного закрепления «ноосферы компьютерных технологий» - программные коды компьютерных продуктов, изготовленных по государственному заказу, должны находиться в открытом доступе чтобы служить основой для других компьютерных разработок, которые свободно может использовать каждый гражданин.

Необходимость поддержки экспортоориентированного бизнеса государством, предоставление исключительных преференций и избавление от налогового бремени.

Проведение государственными структурами, чья деятельность направлена на развитие внешнеэкономических отношений, активных маркетинговых кампаний на международных выставках и конференциях по привлечению иностранных инвестиций.

Предоставление иностранным инвесторам гарантий надежной защиты их прав, налоговых льгот и юридической поддержки в обмен на обязательное регулярное обучение персонала, бесплатное обеспечение программным обеспечением такие учреждения как школы, больницы, музеи и тп.

Необходимость обеспечения государством информационной, маркетинговой и юридической поддержки малым и средним предприятиям, ориентированным на экспорт компьютерных технологий.

## **Обнаружение аномалий сети на основе вейвлет-пакетов и ARX-модели**

**Тишина Н.А.**

**ГОУ ВПО «Оренбургский государственный университет»  
Оренбург, Россия**

Предложена модель и алгоритмы идентификации аномальной активности сети на основе прогнозирования состояния трафика с помощью вейвлет-пакетов и ARX-модели.

## **Anomaly detection network based on wavelet-packets and ARX-model**

**N.A. Tishina**

**The Orenburg state university**

The model and algorithms of identification of abnormal activity of a network on the basis of forecasting of a state of the traffic by means of wavelet-packets and ARX-model is offered.

Обнаружение аномалий является на сегодня активно развивающимся методом систем обнаружения и предотвращения вторжений (IDS и IPS). Среди направлений в развитии данного метода – понижение количества ложных тревог, свойственных данному методу и обеспечение работы в режиме реального времени.

Для математического моделирования сетевого трафика с целью обнаружения вторжений в инфраструктуру сети представляется перспективным использовать теорию мультиразрешающего анализа (МРА), основой которой являются методы вейвлет – преобразований и теорию идентификации динамических систем, одной из широко применяемых параметрических моделей в которой является авторегрессионная модель (ARX-модель).

*Моделирование нормального трафика* сети состоит из двух этапов: вейвлет-разложение и построение ARX-модели.

Трафик сети представляется в виде совокупности сигналов – характеристик трафика, рассчитанных за определенный интервал времени.

В ходе вейвлет-разложения сигналы, представляющие трафик сети преобразуются в набор коэффициентов с помощью одного из быстрых алгоритмов кратноразрешающего анализа – вейвлет-пакетов (БВП). БВП позволяют наиболее полно выделить локальные особенности трафика –

всплески и аномалии за счёт дополнительной декомпозиции высокочастотных составляющих спектра сигнала, представляющего трафик.

Предварительная фильтрация трафика позволяет улучшить прогноз за счёт удаления шума. В результате вейвлет-коэффициенты будут приближенно представлять сигнал, который может использоваться для характеристики ожидаемого поведения сетевого трафика.

Далее на основе полученных коэффициентов строится прогнозирующая ARX-модель. Полученная ARX-модель используется для обнаружения аномалий следующим образом: строится ARX-модель, характеризующая нормальное состояние трафика сети и вычисляется погрешность для текущего трафика  $y(t)$ , если на вход будет поступать нормальный трафик, то погрешности будут небольшими, в противном случае будут значительными в месте аномалии.

Представлены алгоритмы обнаружения аномалий на основе предложенной модели.

В результате экспериментальных расчётов установлены значения  $p$  и  $q$  ARX-модели, равные  $p=q=7$ .

Принятие решения о присутствии аномалии проводится согласно методике, направленной на уменьшение количества ложных тревог.

Данная методика обеспечивает минимум среднего риска принятия решений, при ограничении вероятности ложной тревоги на уровне  $p_{\text{ев}} \leq 0,05$ .

Задача повышения производительности метода приводит к разработке параллельных алгоритмов обнаружения аномалий.

Независимые части определяют набор подзадач, которые могут выполняться на многопроцессорных (многоядерных) компьютерах в параллельном режиме, причем образуемые подзадачи не имеют информационных зависимостей, т.е. распараллеливание алгоритмов приведет к увеличению быстродействия метода.

Таким образом, в работе получил развитие метод кратноразрешающего анализа аномального поведения субъектов сети путём обобщения быстрого вейвлет-преобразования гибкой конструкции вейвлет-пакетов с прогнозирующей ARX-моделью. Разработаны алгоритмы идентификации аномальной активности субъектов сети, обеспечивающие работу IDS/IPS в реальном масштабе времени с допустимой достоверностью принимаемых решений.

## **Методика обеспечения безопасности ведения сайтов образовательных учреждений**

**Топчий Андрей Константинович**

**Южно-Уральский государственный университет  
Челябинск, Россия**

## **Methods of protection of web-sites' management of educational organizations**

**Andrew Topchiy**

**South-Ural State University  
Chelyabinsk, Russia**

### **Аннотация**

В данной статье рассмотрена технология обеспечения безопасности web-систем образовательных учреждений на примере официального сайта кафедры «Информационно-аналитическое обеспечение в социальных и экономических системах» ([www.iao.susu.ac.ru](http://www.iao.susu.ac.ru)). Проведён статистический анализ наиболее распространённых атак на web-ресурсы. Рассмотрены наиболее уязвимые места сайта, а так же методология и действия по их защите. Приведена схема реагирования системы на несанкционированный доступ.

### **Annotation**

This article describes the technology of protection educational organizations' web-sites as an example of the official web-site of the department "Information and Analytical Providing of Management" ([www.iao.susu.ac.ru](http://www.iao.susu.ac.ru)). A statistical analysis of the most common attacks on web-resources is taken into account. The article considers the most critical parts of web-sites, methodology and steps for their protection. There is also a scheme of reaction of the system to the unauthorized access.

### **Цели и задачи**

В рамках приоритетного национального проекта «Образование» по программе информатизации образовательного процесса всё большую популярность стало приобретать создание интерактивных web-порталов различных образовательных учреждений. Эти сайты с одной стороны – открытая информационная система для информирования абитуриентов, студентов, и даже предприятий, заинтересованных в данных студентах. С другой стороны – это система с ограниченным доступом к конфиденциальной информации и действиям.

Защищённость информации на подобных ресурсах влияет на многие моменты функционирования, зачастую являясь основополагающим фактором в его существовании и развитии.

В данной работе рассмотрены основные аспекты и методы обеспечения безопасности при ведении сайтов образовательных учреждений на примере официального сайта кафедры «Информационно-аналитическое обеспечение управления в социальных и экономических системах» ([www.iao.susu.ac.ru](http://www.iao.susu.ac.ru)) Южно-Уральского государственного университета.

### **Актуальность**

Тематика данной работы, а именно исследование аспектов информационной безопасности сайта кафедры, включающая в себя методы защиты информации от несанкционированного доступа, соответствует утверждённой 30 сентября 2010 года государственной программе «Информационное общество» в рамках принятой стратегии «Информационные компьютерные технологии для образования и науки» и подпрограмме «Безопасность в информационном обществе».

### **Основные результаты исследования**

Опыт внедрения подобной информационной системы на официальном сайте кафедры «Информационно-аналитическое обеспечение управления в социальных и экономических системах» ([www.iao.susu.ac.ru](http://www.iao.susu.ac.ru)) Южно-Уральского государственного университета показывает, что данная информационная защита позволяет существенно осложнить проникновение хакеров, защитив наиболее узкие места системы (представлены в Таблице 1). Это способствовало снижению количества успешных атак на информационную целостность сайта.

Таблица 1 – Возможные уязвимости отдельных частей сайта

Функциональные части сайта	Возможные атаки
Главная оболочка сайта (CMS система)	XSS, SQL-injection, PHP-injection
Система авторизации пользователей и административные функции	SQL-injection, повышение привилегий
Новостная лента	XSS, SQL-injection, SPAM
Гостевая книга	XSS, SPAM

На Рисунке 1 представлена общая схема реагирования системы на примере официального сайта кафедры «Информационно-аналитическое обеспечение управления в социальных и экономических системах».



Рисунок 1 - Иллюстрация действий системы на несанкционированное воздействие

Система защиты сайта кафедры, основанная на 3 основных подсистемах (разграничение прав пользователей, журнал событий, контроль версий), включает такие методы защиты как фильтрация переменных от запрещённых значений, шифрование активных сессий пользователей, CAPTCHA-проверку полей ввода информации и др.

### Практическое применение в сфере информационной безопасности

Технология защиты, рассмотренная выше, призвана обеспечить оптимальный уровень защиты информации, и может применяться не только на сайтах государственных учреждений, но и на других web-ресурсах.

## Учебный проект для обучения студентов гуманитарных специальностей навыкам обеспечения защиты информации

Филимошин В. Ю.

ГОУ ВПО «Магнитогорский государственный университет»

## The educational project for training of students of humanitarian specialities to skills of maintenance of protection of the information

Filimoshin V. Ju.

Magnitogorsk state university, Faculty of Informatics, 5 course

В современном обществе, практически все пользуются компьютерными технологиями для различных целей. Уровень подготовленности у всех разный и не каждый сможет обеспечить свою информационную безопасность.

Учебный проект «Защита информации: основы» направлен на обучение студентов гуманитарных специальностей, но может применяться и для обучения студентов других специальностей. В данный проект можно добавлять дополнительные игры, практические работы для повышения качества обучения студентов.

**Цель проекта** «Защита информации: основы»: подготовить студентов гуманитарных специальностей к различным ситуациям связанные с угрозой информационной безопасности.

**Задачи** проекта «Защита информации: основы» состоят в следующем:

1. Научить учащихся выявлять мошенников;
2. Научить учащихся обеспечивать информационную безопасность ПК;
3. Научить учащихся защищать данные на съёмных носителях.

После прохождения учебного проекта «Защита информации: основы», учащиеся смогут отличать мошенников от обычных людей, обеспечивать защиту данных с помощью шифрования, составлять «правильные» пароли, защищать свой ПК от потенциально опасных внешних накопителей, «лечить» ПК от вирусов, а также находить выход из стандартных ситуаций, связанных с информационной безопасностью.

In a modern society, practically all use computer technologies for the various purposes. Level of readiness at all different and not everyone can provide the information security.

The educational project «information Protection: bases» it is directed on training of students of humanitarian specialities, but it can be applied and to training of students of other specialities. In the given project it is possible to add additional games, practical works for improvement of quality of training of students.

The project purpose «information Protection: bases»: to prepare students of humanitarian specialities for various situations connected with information security threat.

Project problems «information Protection: bases» consist in the following:

1. To teach pupils to reveal swindlers;
2. To teach pupils to provide information security of the personal computer;
3. To teach pupils to protect the data on demountable carriers.

After passage of the educational project «information Protection: bases», pupils can distinguish swindlers from usual people, provide protection of the data by means of enciphering, make "correct" passwords, protect the personal computer from potentially dangerous external stores, "treat" the personal computer for viruses, and also find a way out of the standard situations connected with information security.

## Интеллектуальная фильтрация несанкционированных рассылок на основе нейронной сети

Чернопрудова Елена Николаевна

ГОУ Оренбургский государственный университет,  
факультет информационных технологий (ФИТ), кафедра ПОВТАС  
[chernoprudovaln@mail.ru](mailto:chernoprudovaln@mail.ru)

Аннотация: в статье рассмотрена модель представления текста «терм-документ», предложена модель нейросетевого классификатора. Определены основные этапы построения данного классификатора.

In article the model of representation of the text "term-document" is considered, a model of neural network classifier. The main stages in the construction of the classifier

В настоящее время проблема несанкционированных рассылок электронных сообщений (спама) очевидна. В Правилах оказания телематических услуг связи (Постановление Правительства Российской Федерации от 10.08.2007 № 575) дается определение спама, как телематического электронного сообщения, предназначенного неопределенному кругу лиц и доставленное абоненту или пользователю без их предварительного согласия.

Анализ решений, связанных с системами противодействия несанкционированным рассылкам, показал преобладание фильтров, построенных на байесовском подходе. Как известно, этот метод не позволяет учитывать семантику электронных сообщений, т.е. системы фильтрации входящих сообщений неполно используют современные методы искусственного интеллекта для решения задачи классификации. Отсюда, развитие методов и алгоритмов фильтрации спама является актуальной задачей.

В данной статье задача фильтрации несанкционированных рассылок электронных сообщений сведена к автоматической классификации текстов. Первым этапом решения задачи автоматической классификации текстов является преобразование документов, имеющих вид последовательности символов, слов либо устойчивых словосочетаний к виду, пригодному для алгоритмов машинного обучения в соответствии с задачей классификации. Таким образом, любой документ можно описать в виде точки в  $M$  – мерном пространстве.

Отдельной задачей при преобразовании текста в вектор является вычисление весов признаков. Анализ источников посвященных данной тематике показал, что наиболее оптимальным для определения веса является следующая мера взвешивания:

$$w_{ij} = \frac{\log(f_{ij} + 1) \log\left(\frac{M}{M_j}\right)}{\sqrt{\sum_{j=1}^N \left[ \log(f_{ij} + 1) \log\left(\frac{M}{M_j}\right) \right]^2}}$$

где  $f_{ij}$  - частота термина  $j$  в спам-сообщении  $i$ ,

$M$  - число сообщений в выборке,

$N$  - число термов в выборке после удаления служебных слов,

$M_i$  - общее число сообщений, содержащих терм  $i$ .

Получаемое пространство признаков имеет большую размерность, что требует больших вычислительных затрат и результаты становятся ненадежными из-за недостатка обучающих выборок. Поэтому необходимо сокращение первоначального набора признаков. Оптимальным методом сокращения размерности информативной матрицы определен метод  $\chi^2$ . Анализ основных методов классификации текста показал, что наиболее перспективным направлением исследований в

области фильтрации и классификации текста и электронных сообщений являются нейросетевые методы, основными достоинствами которых являются: возможность анализа данных в условиях неполноты, искаженности и неточности информации, а также работа в режиме реального времени. В качестве нейросети для решения задачи фильтрации несанкционированных рассылок предложена адаптивная двухслойная нейросеть, так как она позволяет проверить, соответствует ли «новый» образ поступивший на вход нейронной сети «старому», что нельзя выполнить другими типами нейронных сетей. В качестве классификатора выбран классификатор Гроссберга, классификация документов сводится к предъявлению обученной нейронной сети вектора анализируемого текста и поиска значений соответствия образов, выбор образца с наибольшим соответствием. При использовании в качестве входных векторов текста в виде лексических векторов модели терм-документ, входной слой содержит столько нейронов, сколько терминов в словаре обучающей выборки документов ( $N_{ij}$ ), весовые вектора  $W_i$  нейронов распознающего слоя содержат вес  $w_{ji}$   $j$ -ого термина для  $i$ -ого класса

Таким образом, модель нейросетевого классификатора интегрированная с моделью «терм-документ» значительно упрощает обучение и классификацию, не требует больших вычислительных ресурсов. Следует также отметить, что предложенная модель построенного нейросетевого классификатора не ограничивается изложенными в статье методами, но является перспективным направлением в области решения задач интеллектуальной фильтрации несанкционированных рассылок.