Заключительный уровень – уровень практического применения является естественным продолжением решений, принятых на уровне управления организацией и методик, внедренных на уровне управления группами и их взаимодействием. На уровне управления исполнителями воплощается идеология и подходы, принятые для всей организации. В идеале этот блок завершается созданием самообучающейся организации [2].

Подводя итоги, следует сказать, что кардинальные изменения, происходящие в экономике, развитии сферы туризма, развитии средств производства, на рынке труда меняли взгляд на персонал организации. Персонал превратился в ключевой ресурс и капитал современной организации, от которого зависит ее успешность и эффективность.

За время своего существования службы по управлению человеческими ресурсами существенно расширили направления своей деятельности и увеличили степень участия в делах организации. Поэтому управление человеческими ресурсами превращается в мощный современный инструмент профессиональной работы с персоналом. Выделение управления человеческими ресурсами в особую функцию и применение системного подхода к этой деятельности способствует организации в достижении ее целей, способствует росту конкурентоспособности.

Современные методы управления человеческими ресурсами помогают туристским предприятиям максимально эффективно использовать потенциал каждого сотрудника на фоне роста удовлетворенности работников своим трудом, с учетом специфики данной отрасли.

Источники и литература:

1. Армстронг М. Стратегическое управление человеческими ресурсами / Армстронг М. – М. : Инфра, 2002. – 328 с. (Серия "Менеджмент для лидера")
2. Армстронг М. Практика управления человеческими ресурсами / Армстронг М. – 10-ое изд. – СПб. : Питер, 2009. – 832 с
3. Зайцева Т. В. Модель управления человеческими ресурсами организации // Вестник Московского университета. Сер. 21. Управление (государство и общество). – 2007,№ 2. – Режим доступа к журналу : http://mars.arbicon.ru/?mdl=journal_info&id_journal=654
4. Каплан Роберт С. Сбалансированная система показателей. От стратегии к действию / Каплан Роберт С., Нортон Дейвид П. ; [Пер. с англ. М. Павлова]. – М. : ЗАО «Олимп-Бизнес», 2004. – 304 с.
5. Механизм организации новой системы стимулирования персонала предприятия [Электронный ресурс] / Любый А. В. – Режим доступа : http://infomanagement.ru/avtorskie_statiy/1
6. Эдвинссон Л. Корпоративная долгота. Навигация в экономике, основанной на знаниях / Эдвинссон Л. – М. : ИНФРА–М, 2005. – 248с.

Ивченко А.С., Пенькова И.В. **УДК 004.738.5**

АНАЛИЗ ПРИМЕНЕНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье проведено исследование степени защиты операционных систем и других компьютерных программ от угроз информационной безопасности с применением современного антивирусного программного обеспечения. Проведено сравнение основных наиболее известных антивирусных программ по предварительно определенным критериям.*
Ключевые слова: *информационная безопасность, антивирусное программное обеспечение, информационные технологии.*

Анотація. *У статті проведено дослідження ступеня захисту операційних систем і інших комп'ютерних програм від загроз інформаційної безпеки із застосуванням сучасного антивірусного програмного забезпечення. Проведено порівняння основних найбільш відомих антивірусних програм за заздалегідь визначеними критеріями.*
Ключові слова: інформаційна безпека, антивірусне програмне забезпечення, інформаційні технології.

Summary. *The paper investigates the protection degree of operating systems and other software from security threats using modern anti-virus software. There have been comparied the best-known anti-virus programs on predetermined criteria. The analysis and researches of anti-virus software gave possiblities to come to the following conclusions:*
not every modern antiviruses is able to resist even to the morden threats to the informative safety, or not able to resist them at sufficient level.
It is possible to consider Kaspersky Laboratory as the most effective antivirus, because he is able to prevent basic threats and can educe most of viruses and trojan programs.
For development of antiviruses competitiveness with lower level of defence it is necessary to develop the greater amount of protective components, and also to trace regularly and react on appearance of new modern threats of informative safety.
Keywords: *information security, anti-virus software and information technology.*

Актуальность. Для современных предприятий, компаний или организаций одной из главных задач является обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Повреждение, утечка, неимение и кража информации – это всегда убытки для каждой компании. Например,

могут появиться убытки от плохой репутации компании, от отсутствия клиентов, от затрат на возобновление стабильной работы или от потери важной информации, которой располагала данная компания.

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность.

1. Целостность данных – защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных. Примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании.
2. Конфиденциальность информации – незаконное разглашение, утечка, повреждение информации;
3. Доступность информации для всех пользователей – отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

Одним из способов обеспечения информационной безопасности является антивирусное программное обеспечение, роль которых в информационной безопасности проанализирована в данной работе.

Анализ основных публикаций. Вопросам обеспечения информационной безопасности, в том числе и с использованием антивирусного программного обеспечения посвящены труды многих отечественных и зарубежных ученых: И. Безруков [1; 2], В. Пярин, А. Кузьмин, С. Смирнов [3], В. Дрожиннов, А. Штрик [4], Дж. Уайт, Дж. Лонг [5], К.Кирби [6]. Однако проведенный анализ показывает, что данная информация очень быстро устаревает, поэтому требуется постоянное обновление актуальной информации.

Цели и задачи. Целью настоящего исследования является детальное изучение наиболее известного антивирусного программного обеспечения как средства информационной безопасности. Результаты исследования дадут возможность оценить степень обеспечения информационной безопасности с использованием антивирусов, выявить наиболее конкурентоспособные и надежные антивирусы, а также определить направления и ориентиры для дальнейшего развития антивирусного программного обеспечения.

Основной материал исследования. Антивирусы являются одним из самых эффективных средств защиты против угроз информационной безопасности. Если операционная система не будет обеспечена защитой антивирусной программы, может произойти заражение вредоносными программными объектами, что в конечном итоге повлечет за собой угрозу информационной безопасности [2]. Сегодня мы можем видеть достаточно большой спектр угроз информационному бизнесу в сфере информационных технологий.

Для того, чтобы проанализировать надежность и степень защиты антивирусов, необходимо рассмотреть основные угрозы, которые могут присутствовать в сфере информационных технологий [7]. В таблице 1 рассмотрены основные угрозы информационному бизнесу в сфере информационных технологий.

Таблица 1. Угрозы информационной безопасности в сфере IT

Название угрозы	Угрозы информационной безопасности	Нарушение одного из критериев ИБ
Вирусы	Нарушение работы компьютера. Удаление файлов. Приведение в недееспособность структур размещения данных Блокирование работы пользователя. Способность создавать копии самого себя.	Конфиденци-альность Целостность Доступность
Шпионские программы (spyware)	Незаконная установка на компьютер без разрешения владельца с целью сбора конфиденциальной информации о пользователе и о его пользовательской активности.	Конфиденци-альность
DdoS-атака	Невозможность пользователя получить доступ к серверу, на который произведена DdoS-атака.	Доступность Целостность
Фишинг	Обманным путем (например, создание поддель-ного веб-сайта или массовая рассылка писем) заставляет пользователя раскрыть свои персональные данные: логин, пароль, парольные фразы, PIN-коды от банковских и SIM-карт и др.	Конфиденци-альность
Спам (например, рассылка писем, содержащих компьютерные вирусы)	При получении письма со ссылкой и при нажатии на нее, начинается скачивание неизвестного файла (например, архива), который является вирусом. Нарушение работы компьютера. Удаление файлов. Приведение в недееспособность структур размещения данных Блокирование работы пользователя.	Конфиденци-альность Целостность Доступность
Кейлоггеры	Перехват информации, набираемую пользовате-лем на клавиатуре в данный момент времени. Получение незаконного доступа к логинам и паролям от соцсетей, форумов сайтов и др. Получение незаконного доступа к данным кредитных карт.	Конфиденци-альность
Троянские программы	Реализация незаконных действий, не подтверж-денных пользователем: кража, блокирование, уничтожение конфиденциальной информации. Нарушение нормального функционирование компьютера, впоследствии возможно потеря некоторой важной информации.	Целостность Конфиденци-альность Доступность

Также для полноценного анализа антивирусных программ необходимо определить основные общие известные методы борьбы с вирусами.

При поиске и уничтожении известных вирусов наиболее распространенным является метод сканирования. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая база данных сканирования с фрагментами кодов известных компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования [8]. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются сканерами или детекторами. Программы, включающие функции восстановления зараженных файлов, называют полифагами (фагами), докторами или дезинфекторами. Принято разделять сканеры на следующие:

- транзитные, периодически запускаемые для выявления и ликвидации вирусов;
- резидентные (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить только те вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура [1]. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код [5]. Это затрудняет или делает невозможным выделение сигнатуры и, следовательно, обнаружение вирусов методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Таким образом, вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключается в проверке и сравнении текущих параметров вычислительной системы с эталонными параметрами, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не является прерогативой системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификаций и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые ревизорами. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут «только для чтения» файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков [6]. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем (в частности исторический профиль сетевого трафика), которые сравниваются с текущими параметрами.

Ревизоры, как и сканеры, делятся на транзитные и резидентные. К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими различные неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Следовательно, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для лечения файлов, зараженных неизвестными вирусами, обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемый вакцинацией [8]. Идея метода состоит в присоединении к защищаемой программе модуля (вакцины), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяют выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код, устанавливающий резидентный

модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют эвристическим анализатором.

Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средств: программы-фильтры; аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания с целью контроля подозрительных действий. При этом они могут блокировать «опасные» действия или выдавать запрос пользователю.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует все обращения к дисковой подсистеме компьютера. Это не позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, «опасные» операции и т.д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

К недостаткам указанных контроллеров, таких как ISA-плат, относят отсутствие системы автоконфигурирования, и, как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными.

При работе в глобальных сетях общего пользования, в частности в Internet, кроме традиционных способов антивирусной защиты данных компьютеров, становится актуальным антивирусный контроль всего проходящего трафика. Это может быть осуществлено путем реализации антивирусного прокси-сервера, либо интеграции антивирусной компоненты с межсетевым экраном. В последнем случае межсетевой экран передает антивирусной компоненте (или серверу) допустимый, например, SMTP, FTP и HTTP-трафик. Содержащиеся в нем файлы проверяются на предмет наличия вирусов и, затем, направляются пользователям. Можно сказать, мы имеем дело с новым уровнем антивирусной защиты - уровнем межсетевого экранирования.

Для анализа степени защиты антивирусных программ были выбраны следующие программные продукты: Антивирус Касперского, Dr.Web, Eset, Avast, Каждый из продуктов подробно изучался, подвергался различным видам вирусных атак. Исходя из исследований, мы получили следующие данные о каждой антивирусной программе:

1. Антивирус Касперского разрабатывается в Российской Федерации. Первый релиз данного антивирусного программного обеспечения был произведен в 1997 году. Антивирус имеет достаточно широкий спектр действия, проявил себя на достаточно высоком уровне. Антивирус Касперского отслеживает шпионские программы. Также при появлении спама немедленно его проверяет и блокирует. Данный антивирус определяет и блокирует различного рода клавиатурные перехватчики, предотвращает Ddos-атаки. Проявил достаточный уровень борьбы с фишингом. Антивирус Касперского распознает и блокирует около 85% троянских программ и 88% предотвращения вирусов от общего количества. Это является наиболее высоким показателем среди рассмотренного программного обеспечения. Недостатком данной программы являются достаточно высокие системные требования и значительное занижение быстродействия операционной системы (особенно на недостаточно мощных компьютерах).
2. Dr.Web так же, как и Антивирус Касперского производится в Российской Федерации. Первая версия антивируса выпущена в 1992 году. В основном его защита направлена на обеспечение безопасной работы в сети интернет. Имеет менее высокую степень защиты информации. Dr.Web достаточно эффективно определяет и блокирует шпионские программы. Со спамом способны бороться не все версии данного антивируса, так же, как и с фишингом. Во всех версиях присутствует защита от клавиатурного перехватчика. Антивирус на достаточном уровне справляется с Ddos-атаками. Dr.Web предотвращает около 47% от общего количества вирусов и улавливает около 51% троянских программ, что является недостаточно высоким показателем. Недостатком является узкая направленность защиты.
3. Антивирус фирмы Eset разрабатывается и производится в Словакии. Первый релиз данного антивируса произошел в 1987 году. Eset на высоком уровне борется со шпионскими программами, также с фишингом. Данный антивирус абсолютно не определяет и не предотвращает спам, не имеет в себе такого компонента, как защита от клавиатурных перехватчиков. Зато на достаточном уровне борется с Ddos-атаками. Eset определяет и блокирует около 24% троянских программ и 29% вирусов от общего количества. Это наиболее низкий показатель среди четырех отобранных программных средств. Недостатком является слабый уровень защиты и малое количество защитных компонентов.
4. Avast антивирус выпускается в Чехии с 1995 года.

Не все версии данного антивируса способны распознавать и нейтрализовать шпионские программы, а также фишинг и Ddos-атаки. На высоком уровне присутствует борьба со спамом и защита от клавиатурных перехватчиков. Avast предотвращает 41% вирусов и 49% троянских программ от общего количества, что является средним показателем среди рассмотренных. Недостатком является – малое разнообразие защитных компонентов.

Подводя итог анализа всех четырех рассмотренных антивирусных продуктов, составим таблицу 2.

Таблица 2. Действие антивирусов против угроз информационной безопасности*

Антивирус	Шпионские программы	Спам	Фишинг	Вирусы	Клавиатурный перехватчик	Ddos-атака	Троянские программы
Касперского	Да	Да	Да	88 %	Да	Да	85 %
Dr.Web	Да	±	±	47 %	Да	Да	51 %
ESET	Да	Нет	Да	29 %	Нет	Да	24 %
Avast!	±	Да	±	41 %	Да	±	49 %

** - обозначение «±» трактовать, как «не все версии»*

Выводы. Исходя из анализа и исследований антивирусного программного обеспечения можно сделать следующие выводы:

Не все современные антивирусы способны противостоять даже известным на данный момент угрозам информационной безопасность, либо не способны им противостоять на достаточном уровне.

Наиболее эффективным антивирусом можно считать Лабораторию Касперского, так как он способен предотвратить основные угрозы и может выявить наибольшее количество вирусов и троянских программ.

Для развития конкурентоспособности антивирусов с более низким уровнем защиты необходимо разрабатывать большее количество защитных компонентов, а также регулярно отслеживать и реагировать на появление новых современных угроз информационной безопасности.

Источники и литература:

1. Безруков И. Н. Компьютерная вирусология: справочное пособие. / И. Н. Безруков. – Киев, 1991.
2. Безруков И. Н. Технология применения средств защиты от вирусов / И. Н Безруков // Вычислительная техника и ее применение.– 1991. – №7.
3. Безопасность электронного бизнеса. / В. А. Пярин, А. С. Кузьмин, С. Н. Смирнов. – М., Гелиос-АРВ, 2002.
4. Дрожиннов В. А. Состояние и развитие рынка ИКТ в России / В. А. Дрожиннов, А. Н. Штрик. // Компьютерная неделя. – 2004. – №1(415).
5. White G., Long J. (2010). Global information security factors. International Journal of Information Security and Privacy (IJISP), 4(2), 2010. P. 49–60.
6. Kirby C. Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in Cybersecurity", 2005
7. International Legal Issues Of Cyber Attacks. – [Электронный ресурс]. – Режим доступа : http://perry4law.co.in/cyber_security.
8. European Cybercrime Centre. – [Электронный ресурс]. – Режим доступа : https://www.europol.europa.eu/ec3.

Максимюк Г.М. **УДК 331.101**

ДОСЛІДЖЕННЯ ІСТОРИЧНОЇ ЕВОЛЮЦІЇ КАТЕГОРІЙ, ЩО ХАРАКТЕРИЗУЮТЬ ТРУДОВИЙ ВНЕСОК ПРАЦІВНИКІВ ПІДПРИЄМСТВА

Анотація. *У статті розглянуті основні категорії, що визначають трудовий внесок працівників підприємства (робоча сила, економічно активне населення, трудові ресурси, трудовий потенціал, людський капітал). Виявлено основні вехі їх історичного розвитку, досліджено їх сутність, проведено аналіз підходів вітчизняних та закордонних вчених до визначення сучасних категорій, що характеризують трудовий внесок працівників. Запропоновано схему, яка ілюструє ємність цих категорій.*

Ключові слова: *робоча сила, трудові ресурси, трудовий потенціал, людський капітал.*

Аннотация. *В статье рассмотрены основные категории, определяющие трудовой вклад работников предприятия (рабочая сила, экономически активное население, трудовые ресурсы, трудовой потенциал, человеческий капитал). Исследовано эволюционное развитие этих категорий. Проведен анализ работ отечественных и зарубежных ученых в части значений, которые они придают этим категориям. Проиллюстрировано емкость показателей, характеризующих вклад работников предприятия.*

Ключевые слова: *рабочая сила, трудовые ресурсы, трудовой потенциал, человеческий капитал.*

Summary. *In current conditions of economic activity, economic environment development and interrelation person's role in production changed greatly. In any conditions, in different political and economic eras, within different systems human resources were decisive in reaching goals. Rapid development of theories regarding the role of employees in meeting company's target cased the choice of the issue and its topicality.*

Main categories, defining labor impact of company's workers were examined (work force, gainfully occupied population, manpower, labor potential, human capital). Evolution of these categories was studied. Works of domestic and foreign scientists in the part of meanings, they give to these categories, were analyzed. Capacity of the categories characterizing employees' labor impact was illustrated.

Having studied the categories, characterizing employees' labor impact, we can assert that in the course of time and due to development of economic views on human role in production, one category gave rise to other, more capacious and up-to-date.