Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

УДК 004.056.5

Костеневич
Егор Петрович

РИСКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ ИНТЕРНЕТА

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологии

1 - 59 81 01 Управление безопасностью производственных процессов

Е.П. Костеневич

Заведующий кафедрой ИПиЭ
Константин Дмитриевич Яшин
кандидат технический наук, доцент

Научный руководитель
Тамара Владимировна Казак
доктор психологических наук, профессор

Минск 2015
64

ВВЕДЕНИЕ

В связи с массовой информатизацией современного общества все большую актуальность приобретают знания о способах обеспечения безопасности при использовании средств новых информационных технологий в повседневной практической деятельности. Основной причиной потерь, связанных с компьютерами, является недостаточная образованность в области безопасности.

Под информационной безопасностью понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Цель информационной безопасности – обезопасить систему, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

Несмотря на очевидную важность обеспечения персональной информационной безопасности пользователя Интернета, этому вопросу посвящено незначительное число публикаций и исследований. Большее внимание принято уделять информационной безопасности предприятий и государства, которая может напрямую зависеть от информационной безопасности конкретного пользователя сети Интернет.

Объектом исследования данной работы является пользователь сети Интернет, предметом исследования – средства защиты и методы предотвращения угроз информационной безопасности. Целью магистерской диссертации поставлена выработка рекомендаций по увеличения уровня персональной информационной безопасности пользователя Интернета. Для достижения поставленной цели были выработаны следующие задачи

- изучение наиболее популярных средств защиты и методов предотвращения угроз персональной информационной безопасности пользователя Интернета;
- определение объективных критериев оценки выбранных средств и методов;
- проведение сравнительной оценки изученных средств и методов;
- разработка рекомендаций по применения выбранных средств и методов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель диссертационного исследования – выработка рекомендаций по увеличения уровня персональной информационной безопасности пользователя Интернета.

В соответствии с целью были поставлены следующие задачи исследования:

- изучение наиболее популярных средств защиты и методов предотвращения угроз персональной информационной безопасности пользователя Интернета;
- определение объективных критериев оценки выбранных средств и методов;
- проведение сравнительной оценки изученных средств и методов;
- разработка рекомендаций по применения выбранных средств и методов.

Теоретическая и практическая значимость диссертационной работы состоит в углублении и конкретизации знаний в области информационной безопасности. Исследование по теме, позволяет выявить тенденции в развитии информационной безопасности. Полученные данные могут быть использованы в качестве теоретико-методологической базы для дальнейшего исследования представленных проблем.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам и пользователям информации.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Подход к проблемам информационной безопасности необходимо начинать с выявления субъектов, заинтересованных в обеспечении:

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость, ее защищенность от разрушения и несанкционированного использования. Конфиденциальность – это защита от несанкционированного доступа к информации.

Появление сетевых технологий, развитие глобальных компьютерных сетей, изменило характер проблем защиты, привело к распространению новых угроз безопасности.

Угроза безопасности – потенциально возможное событие, действие, процесс, явление, которое может привести к нанесению материального морального и иного ущерба защищаемому объекту системы.

В современном мире большинство пользователей не знают, как устроен Интернет. Для пользователя все просто – он набирает в строке браузера адрес и попадает на интересующую его страницу. Сколько точек и сервисов при этом задействовано для выполнения этого вызова, пользователя не интересует.

Принципиальная особенность современной ситуации заключается в том, что важнейшей задачей сегодня становится защита информации в компьютерных сетях.

Широкое внедрение компьютеров во все виды деятельности, постоянное наращивание их вычислительной мощности, использование компьютерных сетей различного масштаба привели к тому, что угрозы потери конфиденциальной информации в системах обработки данных стали неотъемлемой частью практически любой деятельности.

Компьютерная защита – это постоянная борьба с глупостью пользователей и интеллектом хакеров. Хакеры чаще всего используют именно некомпетентность и халатность пользователя, что можно считать главной угрозой безопасности.

Лучшая защита от нападения – не допускать его. Обучение пользователей правилам сетевой безопасности может предотвратить нападения. Защита информации включает в себя кроме технических мер еще и обучение пользователей.

Компьютерный вирус – небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Антивирус – программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Такие программы бывают специализированными и универсальными.

Основным недостатком антивирусов является сама основа их работы – они выполняют защитную функцию. Проверка файлов и контроль активности производится по заранее известным шаблонам, и принципиально новую версию вируса антивирусы почти никогда не могут остановить.

В обозримом будущем вряд ли стоит ожидать значительного снижения рисков информационной безопасности. Поэтому пользователям стоит внимательнее относится к защите конфиденциальной информации от незаконных посягательств, самостоятельно выбирая средства и методы защиты.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами, которые подразделяют на методы обнаружения и методы удаления вирусов:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита от вирусов.

Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными:

- работают постоянно;
- обнаруживают все вирусы, независимо от механизма их действия;
- блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.

Для оценки эффективности работы было проведено тестирование популярных антивирусных продуктов. Тестирование проводилось на компьютере, работающем под управление операционной системы Windows 8.1. Для тестирования использовалась коллекция из 3732 вредоносных файлов. Для проверки эффективности были выбраны 12 распространенных антивирусов:

- avast! Internet Security 2014,
- avast! Antivirus Free 2014,
- AVG Internet Security 2014,
- AVG Anti-Virus Free 2014
- Avira Internet Security Suite 2014,
- Avira Free Antivirus 2014,
- Comodo Internet Security Premium 6.3,
- Dr.Web Security Space 9,
- ESET NOD32 Smart Security 7,
- Kaspersky Internet Security 2014,
- McAfee Internet Security 2014,
- Norton Internet Security 2014.

Результаты тестирования представлены в таблице 1.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль над информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы, и обеспечивающее защиту автоматизированной системы посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в автоматизированной системе (или вне автоматизированной системы).

Таблица 1 – Результаты тестирования антивирусных программ.

Название антивируса	Процент распознанных файлов		Процент успешно вылеченных файлов
	при хранении	при запуске	
avast! Internet Security 2014	93,4	62	92,3
avast! Antivirus Free 2014	93,4	0	92,2
AVG Internet Security 2014	93,0	0	91,8
AVG Anti-Virus Free 2014	93,0	0	91,8
Avira Internet Security Suite 2014	97,2	73	95,0
Avira Free Antivirus 2014	97,2	73	95,0
Comodo Internet Security Premium 6.3	92,9	95	90,2
Dr.Web Security Space 9	96,4	0	93,2
ESET NOD32 Smart Security 7	97,0	43	94,5
Kaspersky Internet Security 2014	94,1	89	92,1
McAfee Internet Security 2014	98,2	83	96,4
Norton Internet Security 2014	97,5	73	95,2

Результаты тестирования межсетевых экранов представлены в таблице 2.

Таблица 2 – Результаты тестирования межсетевых экранов

Название продукта	Тестируемая операция		
	поверка доступности с помощь команды ping	попытка передачи файла	попытка подключения к удаленному рабочему столу
avast! Internet Security 2014	полная защита	полная защита	полная защита
AVG Internet Security 2014	полная защита	полная защита	полная защита
ESET NOD32 Smart Security 7	частичная защита	полная защита	частичная защита
Kaspersky Internet Security 2014	полная защита	полная защита	полная защита
McAfee Internet Security 2014	полная защита	полная защита	полная защита

Результаты тестирования антивирусных пакетов показывают, что принципиального различия в уровне их эффективности не наблюдается.

Поэтому для обеспечения приемлемого уровня защиты можно использовать любой известный продукт.

Рекомендации по обеспечению информационной безопасности в Интернете:

- использовать антивирус, регулярно его обновлять;
- использовать межсетевой экран;
- регистрировать электронную почту на известных сервисах;
- использовать основной и «черновой» адрес электронный почты;
- соблюдать рекомендации по выбору имени ящика и пароля;
- использовать функцию отображения времени последнего входа в электронной почте;
- проверять точность введенного адреса в адресной строке браузера»
- не переходить по ссылками из писем и сообщений от незнакомых людей;
- использовать лицензионное программное обеспечение;
- для однократного доступа на сайт использовать специальные сервисы, которые позволяют не вводить личные данные;
- стараться сократить количество выкладываемой личной информации в общий доступ;

Для количественной оценки стойкости пароля используют формулу Андерсона:

$$4{,}32 \cdot 10^4 \cdot (k)\frac{M}{P} \leq A^l,$$

где k – количество попыток подбора пароля в минуту, M – время действия пароля в месяцах, P – вероятность подбора пароля. , A^l – мощность пространства паролей (A – мощность алфавита паролей, l - длина пароля). Очевидно, наибольшее влияние на вероятность раскрытия пароля оказывает l – длина пароля.

ЗАКЛЮЧЕНИЕ

Без надежной системы защиты компьютер становится легкой добычей для киберпреступников. Персональный компьютер может стать частью мошеннической сети и использоваться для проведения сетевых атак, шантажа и рассылки спама. Все это может происходить без ведома пользователя.

Использование пиратских версий платных программ могут быть не только заражены вирусами, но и сами по себе быть опасными для пользовательского оборудования и операционной системы.

Выбирая нелегальное программное обеспечение, пользователь получает менее надежный продукт – значительное число пиратских программ содержат в себе уязвимости, эксплуатируемые киберпреступниками для получения доступа к компьютеру. Отсутствие сервиса поддержки со стороны квалифицированных специалистов значительно сужает поле применения используемого программного обеспечения: так, без своевременного обновления антивирусных баз системы антивирусной защиты фактически неэффективны. Нередко под видом бесплатных программ в Интернете распространяются вредоносные программы.

Следует использовать только лицензионное программное обеспечение (либо свободно распространяемое программное обеспечение из надежных источников) – гарантию стабильной работы персонального компьютера и сохранности ваших данных. В случае возникновения вопросов или трудностей в работе с используемыми программами следует обращаться в службу технической поддержки – обладатели легальных копий программного обеспечения имеют такую возможность.

Основной угрозой информационной безопасности является сам пользователь. Однако соблюдая некоторые правила поведения при использовании компьютера и Интернета, можно значительно снизить риски собственной информационной безопасности.