Обзор и сравнение антивирусного программного обеспечения

Курманбай А.К.
aigera_0796@mail.ru

Научный руководитель: Разумников С.В. ассистент
Юргинский технологический институт (филиал)Национального исследовательского Томского политехнического университета

В настоящее время очень актуальна проблема защиты информации. Информация как продукт может продаваться или покупаться, в связи с чем, мы можем сказать, что она имеет свою стоимость. Показатель стоимости может варьироваться в различных пределах, и когда мы говорим об информации, которая может принести высокую прибыль, здесь и возникает проблема, связанная с ее защитой. Говоря о защите, мы можем выделить два основных момента, это потеря ценности информации или ее исчезновение с устройства хранения данных.

Первый момент связан с халатностью владельцев, обладающих какой либо информацией. Второй момент чаще всего происходит из-за сбоев аппаратной части устройств, на которых хранятся данные, или же из-за вирусов, проникших в те или иные устройства.

В статье рассмотрены угрозы для мобильных устройств и способы защиты от них.

Нужно помнить, что смартфон – это полноценный компьютер. Одной из лидирующих платформ мобильных устройств является Android, именно она представляет особый интерес для киберпреступников. Для данной платформы пишется около 97 % от всех существующих образцов вредоносного программного обеспечения для мобильных устройств.

1. Понятие мобильного вируса.

Мобильные вирусы – это небольшие программы, предназначенные для вмешательства в работу мобильного телефона, смартфона, коммуникатора, которые записывают, повреждают или удаляют данные и распространяются на другие устройства через SMS и Интернет.

Компью́терный ви́рус – вид вредоносного программного обеспечения, способного создавать копии самого себяСвязанно это с тем, что пользователь хранит в телефоне огромное количество персональной информации (номера телефонов, данные различных аккаунтов и почты, фото), кроме того, вирусы имеют возможность отправлять SMS и звонить на платные номера.

2. Обзор мобильных вирусов.

Comwar это очень дорогой мобильный вирус. Он рассылает свои копии путем MMS сообщений. Такой мобильный вирус опасен для вашего кошелька только в том случае, когда вы подключили услугу GPRS, потому что без подключения – вирус не может отправлять ничего. Он, конечно, будет пытаться сделать это, но каждый раз будет остановлен сообщением о том, что подключение к сети не удалось, проверьте настройки подключения. Однако когда у вас всегда подключен GPRS-расходы будут колоссальными.

Commwarrior MMS–червь. Распространяется через MMS и Bluetooth. Рассылает MMS–сообщения без ведома владельца. Быстро «сажает» аккумулятор.

Flexispy – первый полнофункциональный шпион, цена которого на сайте создателей составляла 50$: устанавливает тотальный контроль над смартфоном и отсылает злоумышленнику информацию о совершенных звонках и отправленных SMS.

Fontal – этот мобильный вирус, попадая в память смартфона, изменяет шрифты.

Locknut этот вирус заменяет некоторое количество файлов смартфона неработоспособными файлами. В результате этого после выключения телефона (например, при разрядке батареи) летит прошивка. И вам остается только навестить специалистов сервис–центра.

Metal Gear Solid маскируется под установочный файл игры, после активации ищет и отключает антивирусные программы, после чего становится проблематичным вылечить телефон.

Mosquit данный вирус маскируется под игру для телефона, при его запуске начинает рассылать SMS – сообщения.

Pbstealer вредоносное приложение, которое похищает ваши личные данные (данные записной книги) и пытается отправить их через Bluetooth.

Sculler повреждает записную книжку телефона, в связи, с чем все номера придется набирать вручную. Быстро блокирует почти все функции мобильного, остается только возможность использования голосовых операций. Имеется возможность замены всех пиктограмм меню телефона на свои пиктограммы (обычно в виде черепов).

3. Направления развития мобильных вирусов

Существует несколько направлений развития вирусов, по которым действуют вирусописатели.

1. Кража персональной информации.

В данном случае вирусы собирают персональные данные, имеющиеся в телефоне. Вся информация, полученная вирусом, отправляется на сервер злоумышленников, где используется по их усмотрению. Один из самых серьезных вирусов такого плана Android.Geinimi. Попадая в систему, он определяет местоположение смартфона, загружает файлы из Интернета, считывает и записывает закладки браузера, получает доступ к контактам, совершает звонки, отправляет, читает и редактирует SMS–сообщения.

2. Отправка платных SMS–сообщений и звонки на «партнерский номер» без ведома владельца.

В данном случае за отправку сообщения или за звонок списывается серьезная сумма средств с лицевого счета владельца телефона. Разумеется, деньги попадают в руки злоумышленников. Из самых известных подобных угроз можно назвать Android.SmsSend, а также давно известные RedBrowser и Webster для Java–платформы. Они маскируются под различные полезные программы, вызывая тем самым доверие у пользователя.

3. Мошенничество посредством использования систем интернет–банкинга

В данном случае вирус открывает доступ к мобильному приложению для работы с банком или соответствующему веб-сайту, либо перехватывает SMS-сообщения, передаваемые пользователю от систем интернет–банкинга. На мой взгляд, последствия очевидны, это подписка абонента на дорогостоящие контент–услуги или списывание суммы с банковских счетов, блокируя входящие SMS–запросы от банка и скрытно отправляя подтверждающие SMS о переводе денежных средств.

Выделим основные причины распространения мобильных вирусов: уязвимость программного обеспечения; низкий уровень «мобильной» грамотности; отношение владельцев мобильных телефонов к мобильным вирусам, как к проблеме будущего; любопытство (что будет, если я запущу этот файл/игру/программу); несоблюдение элементарных правил безопасности.

4. Методы защиты от вирусов.

На сегодняшний день большинство разработчиков антивирусов для персональных компьютеров стали выпускать мобильные версии антивирусов. Проблемы современных киберугроз решаются мобильными версиями антивирусов «Лаборатории Касперского», "Dr.Web" и других известных производителей антивирусного программного обеспечения.

Существуют также и сетевые решения операторов связи, позволяющие обойтись без установки антивируса на смартфон. Например, сетевая версия антивируса МТС при выходе в интернет с мобильного устройства блокирует зараженные веб–страницы непосредственно на операторском оборудовании. Таким образом, обеспечивается защита на более высоком аппаратно–программном уровне, разработанном по стандартам информационной безопасности для крупных предприятий, финансовых и банковских учреждений.

Проведем сравнительный анализ пяти крупнейших антивирусных компаний:

1. AVG Mobilation Anti–Virus Pro;
2. Dr.Web Mobile Security;
3. Kaspersky Mobile Security;

Выделим категории для сравнения данных антивирусных программ.

1. Фильтр звонков и SMS.
2. Антивирус.
3. Техническая поддержка.

Таблица 1

Фильтрация звонков и SMS

Критерии	AVG Mobilation Anti-Virus Pro	Dr.Web Mobile Security	Kaspersky Mobile Security
“Белый” / “Черный” список номеров	-	+	+
“Белый”/ “Черный” список SMS/MMS	-	+	+
Блокировка буквенных номеров	-	-	+
Функция “Всегда разрешать звонки и SMS для номеров из контактов”	-	+	+

Таблица 2

Антивирус

Критерии	AVG Mobilation Anti-Virus Pro	Dr.Web Mobile Security	Kaspersky Mobile Security

Антивирусный монитор (защита в реальном времени)	+	+	+
Сканирование по требованию	+	+	+
Сканирование по расписанию	+	-	+
Сканирование отдельных файлов и директорий	+	+	+
Сканировать SD-карту при подключении	-	+	-
Веб - защита (блокирование доступа к зараженным сайтам)	+	-	-
Карантин	-	+	-
Использование «облачных» технологий	-	-	+
Автоматическое обновление антивирусных базТ	+	+	+

Из приведенного анализа можно сделать вывод, что наилучшими антивирусами на сегодня являются Dr.Web Mobile Security и Kaspersky Mobile Security.

Таблица 3

Техническая поддержка

Критерии	AVG Mobilation Anti-Virus Pro	Dr.Web Mobile Security	Kaspersky Mobile Security
Руководство пользователя	-	+	+
Техническая поддержка (через личный кабинет/ электронную почту)	+	+	+
Обучающая информация о продукте на сайте производителя	+	+	+
Форум	+	+	+
Поддержка по телефону	+	+	+

Представленное исследование показало, что большинство антивирусов включает в себя фиксированный набор компонентов безопасности:

- антивирусное ядро (сканер и монитор);
- антивор;
- фильтрацию звонков и SMS.

В заключение отметим, что эксперты считают, что на сегодняшний день количество мобильных вирусов ещё не достигло критической точки и опасность заражения телефона довольно мала по сравнению с обычными компьютерными «инфекциями». Нужно призвать проявлять осторожность при обращении с вашим

мобильным телефоном – и тогда наверняка проблема мобильных вирусов не будет представлять для вас ничего страшного.

Также выделим список правил обращения с мобильными устройствами, чтобы избежать возможности заражения вирусами.

1. Пользоваться антивирусными программами.
2. Необходимо соблюдать осторожность при установке всевозможных приложений на ваш смартфон.
3. Не держать Bluetooth постоянно включенным, или используйте скрытый режим.
4. Не запускать незнакомые программы.

Список литературы:

1. Ю.А.Шафрин Информационные технологии. – М.: Лаборатория базовых знаний, 1999 В.В. Качала, Н.М. Качала Основы информатики. – Мурманск: Издательство МГТУ, 1998.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999.
3. С.В. Симонович, Г.А. Евсеев Практическая информатика. – М.: АСТ-Пресс: Инфорком-Пресс, 2000 г.

К вопросу получения экологически чистой продукции

Воронкова М.Н.
dj_rita@mail.ru

Омский государственный технический университет

Применение удобрений в агроценозах является наиболее действенным и сильным фактором в формировании качества урожая. Рациональное использование средств химизации предусматривает правильный выбор доз удобрений, сроков и способов их внесения, позволяющее получить не только высокий урожай, но и исключить риск загрязнения почвы и продукции токсичными элементами и соединениями [1,2,3].

В задачи исследований входило изучить действие и последействие удобрений на качество получаемой продукции, установить функциональные зависимости качества растениеводческой продукции от обеспеченности почвы нитратным азотом (слой 0-40 см), подвижным фосфором (слой 0-20 см) и соотношения этих биогенных элементов в почве (P_2O_5 /N-NO_3).

Для экологической оценки систем удобрения в севообороте определялось содержание нитратного азота и тяжелых металлов в зерне зерновых культур. Содержание нитратов и тяжелых металлов в урожае в связи с особой их вредоносностью, регламентируется предельно допустимой концентрацией (ПДК). Опасность превышения ее объясняется метаболизмом нитратного азота и тяжелых металлов в процессе питания, превращении их во вредоносные для здоровья соединения, обладающие канцерогенными и мутагенными свойствами.

Исследования проводились в длительном стационарном опыте (год закладки 1976) лаборатории агрохимии СибНИИСХ на полях ОПХ “Омское” расположенного в южной лесостепи Западной Сибири. Зернопаропропашной севооборот развернут в