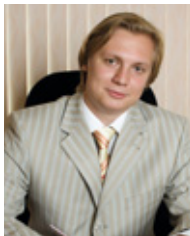




Жуковский
Сергей Евгеньевич,
директор департамента
по работе с силовыми
структурами компании
«Информзащита»



Кадыков
Иван Владимирович,
специалист отдела
технологического развития
продуктов компании
«Код Безопасности»
(ГК «Информзащита»)

Одной из важнейших задач, с которой сталкивается командир любой воинской части Вооруженных Сил, является сбережение конфиденциальной информации используемой в ходе повседневной и боевой деятельности. В силу неуклонности технического прогресса все большая и большая часть такой информации проходит обработку в информационных системах, функционирующих на объектах части. На сбережение этих сведений направлен огромный комплекс усилий ответственных подразделений и должностных лиц. Ежегодно сертифицируются все новые и новые средства и комплексы защиты информации, применяется специализированное программное обеспечение заказной разработки, создающее доверенную программную среду. Все это, казалось бы, раз и навсегда должно предотвратить утечки информации.

В то же время, использование средств защиты информации и специализированного ПО приводит к усложнению работы исполнителей, так как последние лишаются привычных возможностей по использованию обычного общесистемного ПО и возможностей, возникающих при доступе к информационным сетям общего пользования.

В силу того, что, к сожалению, не все сотрудники обладают достаточным уровнем сознательности, весьма распространенной является ситуация, когда сотрудники, ведущие обработку информации в защищенных локальных вычислительных сетях или выделенных помещениях, устанавливают для своего удобства стороннее ПО. Пути его загрузки могут быть самыми разными, от проноса на объект не-

В помощь офицерам ОБИ

разрешенных носителей до установки на объекте беспроводных модемов, широко распространенных в настоящее время на рынке бытовой электроники.

При проведении обследований защищенных объектов специалисты ЗАО НИП «ИНФОРМЗАЩИТА» сталкивались со случаями, когда на корневых удостоверяющих центрах были установлены игры, а на категорированных автоматизированных рабочих местах, прошедших все положенные проверки и исследования, с предустановленной ведомственной операционной системой находились дополнительные грузочные сектора для обеспечения двойной загрузки операционных систем западных производителей и аналогичными не менее примечательными инцидентами безопасности. Таким образом, человеческий фактор обесценивает затрачиваемые на безопасность средства и усилия.

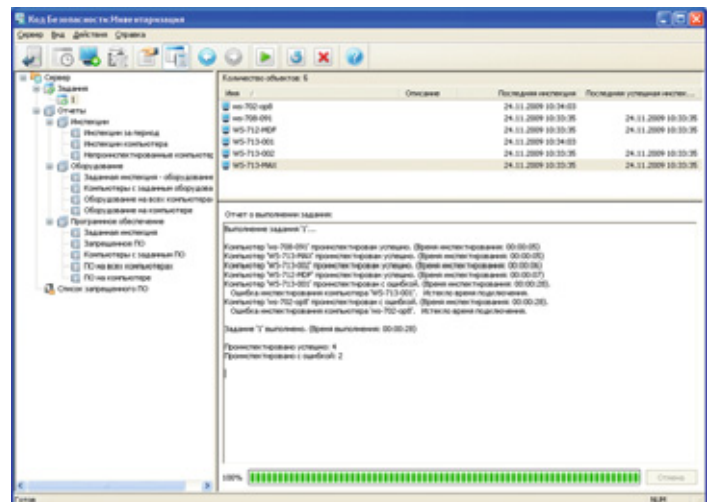
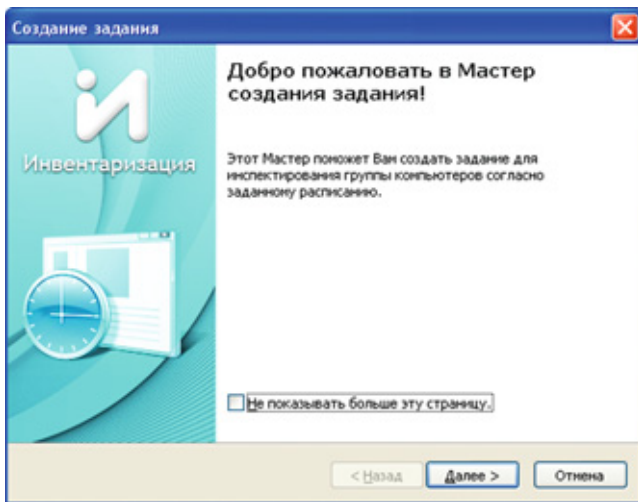
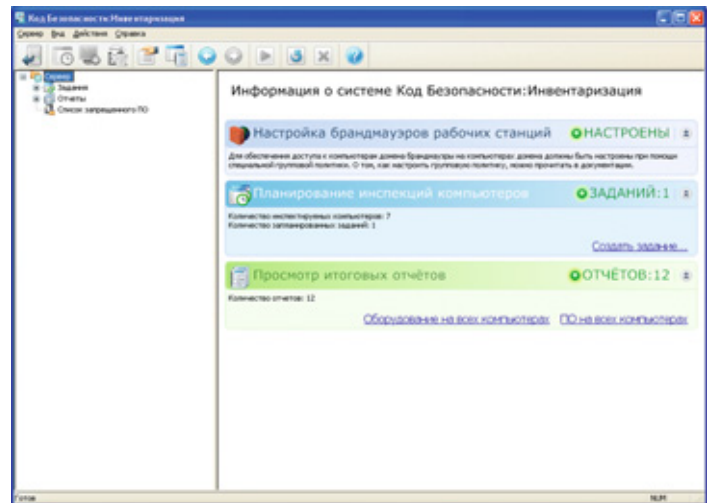
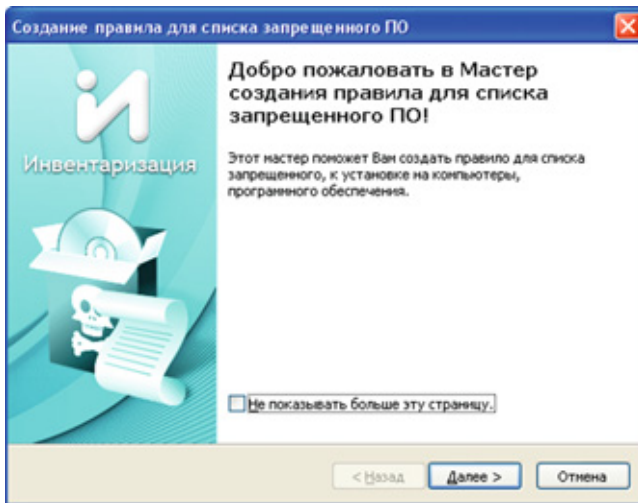
Состояние бесконтрольности используемого программного обеспечения ведет к возникновению многих угроз. Во-первых, при установке модемов это возникновение инсайдерского канала утечки информации, отсутствие злого умысла при создании которого очень сложно доказать. Во-вторых, это санкции регулирующих органов при выполнении проверок при использовании неучтенного ПО. В-третьих, это вирусное заражение с возможностью срыва выполнения решаемых задач. Ну и достаточно экзотическая угроза для силовых структур, но, тем не менее, также возможная — судебное преследование по причине использования нелегального ПО.

Практически во всех ведомствах, осуществляющих обработку конфиденциальной информации, трезво оценивается абсолютная необходимость осуществления контроля за перечнем ПО, установленного на объектах информатизации. Разрабатываются и вводятся в действие различные приказы, инструкции и директивы, предписывающие

использование только определенного списка программного обеспечения, которое необходимо для исполнения служебных обязанностей. Чтобы выполнять такие распоряжения, необходимо регулярно проводить инвентаризацию (аудит) программного обеспечения. Процесс это трудоемкий и требующий высокого уровня подготовки. Зачастую квалификация сотрудников отделов безопасности информации значительно ниже уровня подготовки молодых специалистов в подразделениях информационной направленности, или программно-технические средства, применяемые сотрудниками ОБИ для выявления нарушений, значительно отстают от современных рыночных программных средств. В качестве примера, автор этой статьи во время службы в ВС неоднократно наблюдал, как полковник предпенсионного возраста — сотрудник отдела безопасности информации, вооруженный инструкцией и batch-файлом, запускаемым с дискеты и осуществляющим поиск набора слов и словосочетаний в формате ACSII, пытался выявить факты нелегитимной обработки конфиденциальной информации на компьютере молодого выпускника одного из престижных ВВУЗов, на котором помимо разрешенного комплекта ПО в двойной загрузке была установлена новейшая ОС Windows и самый современный на тот момент пакет офисного ПО, работающего с файлами форматов doc и rtf. Результат был предсказуем. Пример устаревший, но имеющий тенденцию к повторению.

В ходе выполнения инвентаризации необходимо ответить на следующие вопросы:

- Какое количество компьютеров имеется в подразделении?
- Какое программное обеспечение (и версии) используется?
- Какое аппаратное обеспечение?
- Как связать полученные инвентаризационные данные с конкретным сотрудником и его рабочим местом.



После сбора всех данных необходимо провести аналитическую обработку с целью выявления программного обеспечения отсутствующего в формуляре рабочего места и предписании на эксплуатацию, запрещенного регламентом, обеспечивающего связь с мобильными устройствами и предоставляющего возможность модемного соединения. Поэтому воинской части с количеством компьютеров более 50 проведение инвентаризации займёт не один день. От исполнителя требуется квалификация опытного системного администратора.

Для ведения регулярного автоматизированного учета и контроля состава установленного программного обеспечения ПЭВМ и построения отчетов компанией Код Безопасности, входящей в Группу компаний «Информзащита», разработан программный комплекс «Код Безопасности: Инвентаризация». Данный программный комплекс позволяет существенно облегчить и автоматизировать работу офицера, отвеча-

ющего за обеспечение безопасности информации.

«Код Безопасности: Инвентаризация» собирает и накапливает информацию об установленном программном обеспечении воинской части, позволяет создавать отчёты о проведённых инспекциях и помогает выявить нарушителя регламента, в том числе и при наличии второй операционной системы. Принцип действия программы основан на удалённом подключении к реестру инспектируемого компьютера и получении всей необходимой информации. Если компьютер не входит в сеть, для этого специально предусмотрена программа агент, при помощи которой можно провести инвентаризацию. Агент может быть скопирован на любой съёмный носитель и запущен на инспектируемом компьютере. Все собранные сведения помещаются в централизованную базу данных. Не смотря на то, что данное ПО не относится к средствам защиты информации, оно допускается к использованию в автоматизированных

системах класса до 1Г и проверено на НДВ 4. Разрабатываются версии класса до 1В и НДВ 3.

В программе предусмотрена возможность создания списка запрещенного ПО, списки могут конкретизироваться по желанию Заказчика.

С более подробной информацией по данному продукту Вы можете ознакомиться на сайте www.securitycode.ru



Информзащита
Группа компаний

Россия, 127018, Москва, а / я 55
Тел./ факс: (495) 980-23-45
E-mail: defence@infosec.ru
URL: www.infosec.ru