

их развитие. Если же говорить обо всем предприятии, то наибольшее внимание следует уделить внедрению природоохранных и ресурсосберегающих технологий. Что касается охраны атмосферного воздуха, то можно предложить применение более эффективного пылегазоулавливающего оборудования. Главное их достоинство – высокая эффективность очистки при соблюдении оптимальных режимов работы, сравнительно низкие затраты энергии. Проблему утилизации гальванических отходов, можно решить путем организации производства для переработки отходов на территории завода, что значительно снизит экономические затраты.

Следует отметить, что процесс экологизации данного производства будет связан с возрастанием стоимости мероприятий по охране гидросферы и атмосферы. Однако данные затраты компенсируются предотвращением или ликвидированным ущербом, который наносится сбросами.

Учитывая, особую экологическую опасность гальванопроизводства, а также их физический износ и техническую отсталость, можно сделать вывод о том, что главной задачей является устранение особо опасного воздействия на здоровье населения и окружающей среду.

ПОЛИМОРФНЫЕ ВИРУСЫ

Долженков А.А., Грачева Е.В.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: los@pgta.ru

Полиморфизм – высококлассная техника, позволяющая вирусу быть незамеченным по стандартной сигнатуре. Все полиморфные вирусы снабжаются расшифровщиком кода, который по определенному принципу преобразует переданный ему код, вызывая при этом стандартные функции и процедуры операционной системы. Сами методы шифрования могут быть разными, но, как правило, каждая операция имеет свою зеркальную пару. В ассемблере это реализуется очень просто, и таких пар может быть очень много – *ADD/SUB*, *ROL/ROR* и т.п. Немаловажной особенностью полиморфного вируса является то, что вирус содержит операнды, функции и процедуры, которые служат лишь для запутывания кода.

Выделяют несколько уровней полиморфизма, используемых в вирусе:

- самые простые олигоморфные вирусы. Они используют постоянные значения для своих расшифровщиков, поэтому легко определяются антивирусами;

- вирусы, имеющие одну или две постоянные инструкции, которые используются в расшифровщиках;

- вирусы, использующие в своем коде команды-мусор. Это в своем роде ловушка от детектирования, помогает запутать собственный код. Но такой вирус может быть засечен с помощью предварительного отсеивания мусора антивирусом;

- использование взаимозаменяемых инструкций с перемешиванием в коде без дополнительного изменения алгоритма расшифровки, помогает полностью запутать антивирус;

- неизлечимый уровень. Существуют вирусы, которые состоят из программных единиц – частей. Они постоянно меняются в теле и перемещают свои подпрограммы. Характерной особенностью такой заразы являются пятна. При этом в различные места файла записываются несколько блоков кода, что обуславливает название метода. Такие пятна в целом образуют полиморфный расшифровщик, который работает с кодом в конце файла. Для реализации метода даже не нужно использовать команды-мусор, подобрать сигнатуру будет все равно невозможно.

Полиморфизм стал весьма распространенным лишь благодаря расшифровщику. Удобно то, что один

файл может работать со многими вирусами. Этим и пользуются вирусописатели, используя чужой модуль. В полиморфы нередко встраивают код, который выполняется в зависимости от определенной ситуации. Например, при детектировании вируса он может вызвать процедуру самоуничтожения. Как самого себя (частичная или полная безвозвратная модификация кода), так и системы (массовое заражение системных файлов без возможности восстановления). Это очень осложняет поиск антивируса от полиморфного вируса, до антивирусной лаборатории вирус доходит уже в нерабочем состоянии.

Первый полиморфный вирус появился в 1990 году и назывался *Chameleon*. Он вписывал свой код в конец *COM*-файлов, а также использовал два алгоритма шифрования. Первый шифрует тело по таймеру в зависимости от значения заданного ключа. Второй использует динамическое шифрование и при этом активно мешает трассировке вируса. Он не был опасен, хотя содержал в коде ряд ошибок, из-за которых генератор не мог расшифровать тело вируса. При этом исполняемый файл переставал функционировать. После длительного простоя системы *Phantom* выводил на экран видеоизображение с надписью. Она гласила, что компьютер находится под наблюдением опасного вируса.

Параллельно вирусам появлялись и полиморфные генераторы, одним из которых был *MtE*, открывший целые вирусные семейства. Он уже использовал зеркальные функции, чем затруднял своё детектирование. Теперь вирусологу не нужно было писать свой дешифратор, а лишь воспользоваться *MtE*. *MtE*-вирус был перехвачен антивирусной лабораторией, поэтому быстрый выход защиты от первого серьёзного полиморфного вируса защитил множество рабочих станций от заразы.

Другое семейство вирусов *Daemaen* записывает себя в *COM*, *EXE* и *SYS* файлы. С виду эти вирусы выглядят вполне безопасно, но на самом деле происходит запись в *MBR* винчестера и в *boot*-сектора дискета, а тело заразы хранится в последних секторах.

ОЦЕНКА КОНСТРУКТИВНОЙ УСТОЙЧИВОСТИ ОБЩЕСТВЕННО ВАЖНЫХ ЗДАНИЙ ГЕОФИЗИЧЕСКИМИ МЕТОДАМИ

Дробиз М.В., Сотников Д.С.

Балтийский федеральный университет имени Иммануила Канта, Калининград, e-mail: chernaya@bk.ru

Безопасность населения неразрывно связана с объектами жизнедеятельности – общественно важными зданиями и сооружениями. К сожалению, в бурно развивающемся строительном секторе Калининграда в последние годы вопросам экологически безопасного строительства уделяется недостаточное внимание. Землетрясение 2004 года последующими выводами работ комиссий признано своего рода «случайным», хотя ряд прибалтийских сейсмологов рассматривают эти толчки как форшок более мощного события. Таким образом, ни ряд послевоенных зданий, ни современные строения не учитывают сложившиеся реалии.

Для оценки конструктивной устойчивости общественно важных зданий авторским коллективом выбрана методика Ю. Накамуры (Y. Nakamura), согласно которой сейсмометрические исследования оценки уязвимости как архитектурных памятников (Колизей, Пизанская башня), так и множества административных зданий и сооружений (виадуктов, скоростных автомагистралей) успешно выполняются в Японии и ряде стран Евросоюза. В данном методе наблюдения и регистрация микросейсм природного и антропогенного происхождения, в отличие от других методов, требующих сложной и часто дорогостоящей организации, выполняются одиночной трехкомпонентной сейсмологической станцией. При этом не требуется