УДК 622.1:519.7

С.С. Кубрин, Н.Н. Самарин

ОБЕСПЕЧЕНИЕ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ АСУ ТП КОНТРОЛЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА «НЕДЕКЛАРИРУЕМЫЕ ВОЗМОЖНОСТИ РАБОТЫ С ОПЕРАТИВНОЙ ПАМЯТЬЮ»

Проведен анализ рисков аварий на опасных промышленных объектах из-за вредоносного и некорректного программного обеспечения автоматизированных систем управления технологическими процессами. Рассмотрены условия проведения экспертизы промышленной безопасности автоматизированных систем, производящих контроль и управление технологическими процессами. Предложены инструменты, позволяющие производить специализированную экспертизу программного обеспечения на отсутствие в нем недекларированных возможностей». Предложен формальный подход к аудиту использования программным обеспечением оперативной памяти. Разработаны параметры, характеризующие индивидуально характеризующие использование программным обеспечением оперативной памяти.

Ключевые слова: автоматизированные системы, мониторинг, промышленная безопасность, опасные производственные объекты, скрытые угрозы, оперативная память, процессор.

Угольные шахты, разрезы, рудники, и карьеры оснащены современными автоматизированными системами контроля, мониторинга и управления технологическими процессами горного производства. Для обеспечения промышленной безопасности персонала и горных работ предназначены многофункциональные системы безопасности (МФСБ). Основную информацию МФСБ получают через штатные системы мониторинга рудничной атмосферы, состояния массива горных пород, параметров технологического оборудования, системы энергоснабжения и пр. Получаемая информация контролируется и анализируется на предприятии, в объединение и в головном офисе компании. Передача информации осуществляется через производственные, локальные сети горнодобывающего предприятия, корпоративные сети объединения и через глобальную сеть Интернет. Архитектура построения автоматизированных систем в горной промышленности включает три уровня: нижний (чувствительные элементы, датчики, исполнительные механизмы), средний (контроллеры, управляющие станции сбора и передачи данных, программное обеспечение контроллеров), и верхний (приемные коммутирующие устройства, серверная часть и рабочие места операторов, программное обеспечение для серверов и рабочих станций). На сегодняшний день программное обеспечение верхнего и среднего уровня на современном горном предприятии представлено различными разработчиками и в большинстве случаях без исходного кода. В последние годы вошло в практику предоставлять Программный продукт в соответствии с принципом «КАК ЕСТЬ» («AS IS»), при этом запрещается производить декомпилирование и дизассемблирование кода Программного продукта пользователю. Такой подход ведет к тому, что у разработчиков программного обеспечения практически отсутствует ответственность за всестороннее тестирование продукта. Поэтому в современном программном обеспечении по данным Carnegie-Mellon на тысячу строк кода

приходится от пяти до пятнадцати ошибок, которые влияют на его работоспособность. Убытки, возникающие из-за недостаточного отлаженного программного обеспечения по данным Национального Института стандартов и Технологий США, составляют от 22 до 60 млрд долл. в год. Аналогичных статистических данных по РФ нет. Известны случаи, нарушения промышленной безопасности и вывода из строя технологическое оборудование вредоносным программным обеспечением (авария на фабрики по обогащению урана в Ираке из-за компьютерного вируса «Стакснет»). В связи с этим, вызывает озабоченность ситуация, что большая часть базового программного обеспечения, используемого на горнодобывающих предприятиях, в том числе осуществляющее управление промышленной безопасностью, разработана за рубежом. Даже, при отсутствии «злого умысла» у разработчика программного обеспечения существует риск наличия в продукте критических ошибок, которые могут привести к сбою, отказу или выполнению недекларированных действий программным обеспечением автоматизированной системой управления, что особенно опасно в предаварийных и аварийных ситуациях. После ужесточения санкционной политики запада, в сентябре 2014 г. Президент РФ В.В. Путин заявил о необходимости разработок отечественного программного обеспечения. Создания узкоспециализированного универсального программного обеспечения для АСУ ТП долгий и дорогостоящий процесс. В этом случае реальной возможностью обеспечить отсутствие «недекларируемых действий» программного обеспечения является проведение экспертизы.

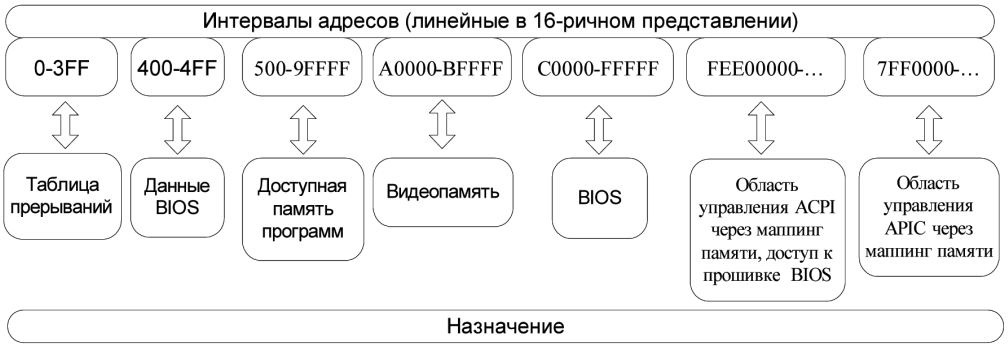
Следует отметить, что в подходе к обеспечению безопасности опасных промышленных объектов сложилась следующая ситуация. Так согласно Федеральному закону № 116 «О промышленной безопасности опасных производственных объектов» о проведении экспертизы промышленной безопасности программного обеспечения не сказано ни слова. В «Правилах проведения экспертизы промышленной безопасности», утвержденных Приказам Федеральной службы по экологическому, технологическому и атомному надзору от 14 ноября 2013 г. № 538 и зарегистрированных в Минюсте РФ 26 декабря 2013 г.требований по проведению экспертизы программного обеспечения систем управления технологическими процессами, мониторинга состояния рудничной атмосферы, массива горных пород, программному обеспечению контроллеров исполняющих команды систем обеспечения безопасности ни каких не предъявляется.

Поэтому, для обеспечения промышленной безопасности горнодобывающих предприятий обязательно необходимо проверить используемое на опасном промышленном объекте программное обеспечение на «недекларированные возможности», которые могут находится в нем, в том числе и из-за не достаточно полного тестирования. Такая проверка возможна только с помощью автоматизированного обнаружения скрытых угроз (дефектов) [1–3], реализуемых программным обеспечением без исходных текстов на основе анализа работы программного обеспечения с различными областями оперативной памяти, устройствами ввода вывода, сетевыми устройствами в виртуальной среде под управлением виртуальной машины. Наиболее актуальным является исследование взаимодействия программного обеспечения с оперативной памятью. В этом случае действия программного обеспечения связанные с записью и выполнением программного кода, расположенного в оперативной памяти являются потенциально опасными, при этом важное значение играет диапазон адресов

оперативной памяти (рисунок). Возможен 21 вариант предварительной оценки действий программного обеспечения с оперативной памятью в зависимости от операции (чтение, запись, выполнение) и используемой областью оперативной памяти. Аудит работы программы в среде виртуальной машины позволяет фиксировать последовательной выполнения операций с оперативной памятью, производимой исследуемым программным обеспечением [2].

Полученную, на основе потактового мониторинга работы процессора, последовательности команд работы с оперативной памятью можно представить в виде конъюнкции выражений, характеризующих вид операции (*R* – чтение, *W* – запись, *X* – выполнение) и области адресного пространства (римская цифра в последовательности приведенной на рисунке. *F* = RI & WIII & & XI & WIV & XI & RII … XII. Соотнося характер (опасно/неопасно) действия с оперативной памятью для каждой области битом, то результат выполнения команды процессора с оперативной памятью в целом характеризуется символом в кодировке KOI-7. Переход к 8-ми битовому представлению (от кодировки KOI-7 к кодировке символов ASCII) осуществляется дополнением семибитовой величины, характеризующей результат выполнения команд процессора нулевым битом слева. Последовательность символов, получаемая в ходе проверки программного обеспечения, полностью характеризуют все операции с оперативной памятью. Свертка по алгоритму бинарной операции сложения дает индивидуальную символьную последовательность, характеризующую работу с оперативной памятью конкретного программного продукта. Оптимальный коэффициент сжатия символьной последовательности, характеризующей операции программного обеспечения с оперативной памятью в целом без потери информативности на основе проведенных многочисленных экспериментов лежит в пределах от 10 до 30.

Таким образом, для обеспечения промышленной безопасности опасных производственных объектов необходимо обязательно производить специализированную экспертизу программного обеспечения на отсутствие в нем «недекларированных возможностей». Наиболее важной, является проверка программного обеспечения по использованию и работе с оперативной памятью. Такая проверка должна производится с помощью инструментов, имитирующих работу процессора – виртуальная машина. Полученный результат потактовых действий программного обеспечения следует представлять в виде байта (семибитовой характеристики потенциальной опасности операций операции с оперативной памятью в



Адресация оперативной памяти

целом дополненной слева нулевым битом). Без потери информативности можно производить свертку полученной последовательности символов по алгоритмы бинарной операции сложения в 10–30 раз. Результат свертки полностью характеризует анализируемый программный продукт по характеру использования оперативной памяти в целом представляет по сути его индивидуальный код суммарной оценки «работы с оперативной памятью».

СПИСОК ЛИТЕРАТУРЫ

1. *Самарин Н.Н., Кубрин С.С.* Анализ надежности программного обеспечения автоматизированных систем управления технологическими процессами горных предприятий от сбоев и вмешательства извне / Материалы 11-й Международной научной школы молодых ученых и специалистов. – М.: ИПКОН РАН, 2014. – С. 150–152.

2. *Кубрин С.С., Самарин Н.Н.* Результаты комплексного анализа программного обеспечения горнодобывающих компаний на недекларированные возможности / Материалы 11-й Международной научной школы молодых ученых и специалистов. – М.: ИПКОН РАН, 2014. – С. 152–154.

3. *Самарин Н.Н., Борисов А.В., Кубрин С.С.* Программный комплекс определенияциклов в областях памяти электронной вычислительной системы с их автоматической регистрацией. Заявка на свидетельство о гос. регистрации программы для ЭВМ, № 16123/0203/ПО от 30.12.2014. ГИАБ

КОРОТКО ОБ АВТОРАХ

Кубрин Сергей Сергеевич – доктор технических наук, профессор, зав. лабораторией,
Институт проблем комплексного освоения недр РАН, e-mail: s_kubrin@mail.ru,
Самарин Николай Николаевич – начальник отдела,
НИИ «Квант», e-mail: samarin_nik@mail.ru.

UDC 622.1:519.7

THE INDUSTRIAL SAFETY PROCESS CONTROL SYSTEM CONTROL SOFTWARE FOR «UNDECLARED CAPABILITIES RANDOM ACCESS MEMORY»

Kubrin S.S., Doctor of Technical Sciences, Professor, Head of Laboratory,
Institute of Problems of Comprehensive Exploitation of Mineral Resources
of Russian Academy of Sciences, 111020, Moscow, Russia, e-mail: s_kubrin@mail.ru,
Samarin N.N., Head of Department, Research Institute «Kvant»,
125438, Moscow, Russia, e-mail: samarin_nik@mail.ru.

The analysis of risks of accidents at hazardous industrial facilities due to malicious or incorrect software of the automated control systems of technological processes. The conditions of carrying out of examination of industrial security of automated systems, manufacturing the control and management of technological processes. The proposed tools to produce the specialized expertise of the software on the absence of undeclared capabilities». Proposed a formal approach to audit use software RAM. Developed parameters that characterize individually characterizing the software to use the RAM.

Key words: automated systems, monitoring, industrial safety, hazardous production facilities, hidden threats, RAM, CPU.

REFERENCES

1. Samarin N.N., Kubrin S.S. *Materialy 11-y Mezhdunarodnoy nauchnoy shkoly molodykh uchenykh i spetsialistov* (Proceedings of 11th International Scientific School for Young Researchers and Specialists), Moscow, IPKON RAN, 2014, pp. 150–152.

2. Kubrin S.S., Samarin N.N. *Materialy 11-y Mezhdunarodnoy nauchnoy shkoly molodykh uchenykh i spetsialistov* (Материалы 11-й Международной научной школы молодых ученых и специалистов), Moscow, IPKON RAN, 2014, pp. 152–154.

3. Samarin N.N., Borisov A.V., Kubrin S.S. *Zayavka na svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 16123/0203/PO* (Application for state registration certificate for computer program no 16123/0203/ПО от 30.12.2014).