DOI: https://doi.org/10.15688/jvolsu10.2016.4.2

УДК 681.326
ББК 67.408

ИССЛЕДОВАНИЕ ВОПРОСОВ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПОЛЬЗОВАТЕЛЯ ПО ДАННЫМ СИСТЕМНОГО РЕЕСТРА

Елена Александровна Максимова

Кандидат технических наук, доцент,
заведующая кафедрой информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Татьяна Александровна Омельченко

Аспирант, научный сотрудник кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Юрий Петрович Умницын

Доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Кристина Петровна Гужаковская

Кандидат физико-математических наук,
доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Существует большое количество подходов к поддержанию требуемого уровня безопасности автоматизированного рабочего места, при этом подходы варьируются по степени их эффективности и стоимостным характеристикам. Использование традиционных активных и пассивных средств защиты информации на предприятии не всегда возможно в силу различных причин. Одним из выходов из сложившейся ситуации может являться постоянный аудит информационной системы как в целом, так и ее отдельных жизненно важных узлов.

Ключевые слова: системный реестр, аудит информационной безопасности, автоматизированное рабочее место, защита информации, внешняя атака.

Аудит информационной безопасности – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций [3].

Важнейшим компонентом ОС Windows, а значит, и автоматизированного рабочего места (далее – АРМ) является системный реестр – сложный, многоплановый механизм, в котором протекают жизненно важные процессы ОС [2], аудит которого необходим для ее безопасного и стабильного функционирования.

Согласно PricewaterhouseCoopers, лидирующие позиции виновников нарушения информационной безопасности занимают действующие сотрудники организации. В первой половине 2015 г. зарегистрировано 954 (65 %) утечки информации, причиной которых стал внутренний нарушитель. В 233 (32 %) случаях она произошла из-за внешних воздействий. Для некоторых случаев (2,6 %) установить вектор воздействия (направление атаки) оказалось невозможно.

В случае внешних атак преступник с помощью вредоносного программного обеспечения (далее – ВПО) ищет уязвимости в информационной структуре, которые могут предоставить ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. Излюбленным местом обитания ВПО являются ключи системного реестра.

В 2015 г. каждый третий компьютер в бизнес-среде был подвергнут хотя бы одной атаке через Интернет. В таблице 1 представлено расположение популярного ВПО в ключах системного реестра.

Локальные угрозы были обнаружены на 41 % компьютеров корпоративных пользователей. Статистика представлена в таблице 2.

Защита ПО от несанкционированного доступа и воздействия вредоносного кода при установке и использовании АРМ пользователя является основной частью общей задачи обеспечения безопасности информации предприятия. Наряду с применением систем защиты информации от вредоносного кода и несанкционированного доступа необходимо выполнение целого ряда мер, которые включают в себя:

– организационно-технические;

– административные мероприятия [4].

Одним из таких мероприятий является обеспечение аудита информационной безопасности по данным системного реестра на установленном АРМ.

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Существует два вида аудита: внешний и внутренний. Аудит информационной безопасности по данным системного реестра на установленном АРМ является мероприятием, которое относится к внутреннему аудиту [1].

Для защиты системного реестра от вредоносных атак необходимо контролировать нежелательные действия, происходящие в реестре во время установки каждой новой программы. Сделать это вручную невозможно, так как реестр содержит миллионы записей. Поэтому необходимо проанализировать существующее внешнее программное обеспечение, предназначенное для аудита информационной безопасности системного реестра на АРМ пользователя (см. табл. 3).

Анализ существующего ПО показал, что имеет место необходимость в создании нового программного комплекса аудита информационной безопасности АРМ пользователя по данным системного реестра.

Программный комплекс должен включать два режима работы:

1. Ручной режим полного аудита системного реестра. Ручной режим включает в себя функцию установки таймера на проведение аудита. Отчетность сохраняется в отдельную базу данных. Минусом данного режима является то, что он слишком ресурсоемкий в плане потребления ресурсов ПК и времени проведения аудита.

2. Решением проблемы большого ресурсопотребления ручного режима является автоматический, выдержанный по времени аудит определенного набора ключей системного реестра. Данный набор будет составляться согласно расположению в ключах реестра актуального ВПО, а также по инициативе специалистов в области информационной безопасности и системных администраторов.

Перед проведением аудиторской проверки необходимо сформировать модель требуе-

мого состояния ключей системного реестра. В общем виде ее можно представить как:

$$F_{ts} = F(X_{ij}), \quad (1)$$

где

$$X_{ij} = (y_{ij}, k_{ij}, z_{ij}), \quad (2)$$

где X_{ij} – требуемые параметры i-го ключа в j-ном разделе системного реестра; y_{ij} – требуемое имя i-го ключа в j-ном разделе системного реестра; k_{ij} – требуемый тип i-го ключа в j-ном разделе системного реестра; z_{ij} – требуемое значение i-го ключа в j-ном разделе системного реестра.

Процесс проведения аудита системного реестра в ручном режиме работы программы описывается следующей моделью:

$$F_{ar}^{*} = F^{*}(X_{ij}), \quad (3)$$

где

$$X_{ij} = (y_{ij}, k_{ij}, z_{ij}), \quad (4)$$

где X_{ij} – полученные параметры i-го ключа в j-ном разделе системного реестра; y_{ij} – полученное имя i-го ключа в j-ном разделе системного реестра; k_{ij} – полученный тип i-го ключа в j-ном разделе системного реестра; z_{ij} – полученное значение i-го ключа в j-ном разделе системного реестра.

В процессе аудиторской проверки происходит сравнение значений ключей требуемого состояния с полученными в ходе проверки данными.

При формировании модели требуемого состояния ключей системного реестра для

Таблица 1

Сводная таблица популярного ВПО, передающегося через Интернет, и его расположения в реестре

№	Название	Атакуемые пользователи, %	Расположение в системном реестре
1	Malicious URL	57,0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunServices HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services
2	Trojan.Script. Generic	24,7	HKEY_LOCAL_MACHINE\SOFTWARE\Classes Ключи реестра, прописывающие работу браузера
3	Trojan.Script. Iframer	16,0	HKLM\SYSTEM\CurrentControlSet\Control\Power\ User\PowerSchemes Ключи реестра, прописывающие работу браузера. HKEY_CURRENT_USER\Software\Microsoft\ Protected Storage System Provider
4	Exploit.script. blocker	4,1	HKEY_LOCAL_MACHINESYSTEMCurrentControl SetControlLsa
5	Trojan.Win32. Generic	2,5	HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon HKEY_USERS \ DEFAULT \ Software \ Microsoft \ Windows \ CurrentVersion \ Internet Settings HKEY_LOCAL_MACHINE \ SYSTEM \ ControlSet001 \ Services \ svflooje \ Enum
6	Net–worm.Win32. kido.ih	2,3	HKEY_USERS\Software\Microsoft\Windows\Current Version\Explorer\Browser Helper Objects HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\CurrentVersion\Ext\Stats
7	Trojan–Downloader. JS.Iframe.dig	2,0	Ключи реестра, описывающие работу браузера
8	Exploit.Script. Generic	1,2	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\policies\Explorer\run\
9	Packed.Multi.Multi Packed.gen	1,0	HKEY_CURRENT_USER\Software\ Microsoft\Protected Storage System Provider
10	Trojan– Dowloader.Script. Generic	0,9	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\ CurrentVersion\Run

проведения аудиторской проверки в автоматическом режиме необходимо учитывать данные таблиц 1 и 2.

$$F_{ts}^{*} = F^{*} \cdot (X_{ij}), X_{ij} \in V, \quad (5)$$

где

$$X_{ij} = (y_{ij}, k_{ij}, z_{ij}), \quad (6)$$

где X_{ij} – требуемые параметры i-го ключа в j-ном разделе системного реестра; V – определенный набор ключей, предназначенный для автоматического режима работы программного комплекса; y_{ij} – требуемое имя i-го ключа в j-ном разделе системного реестра; k_{ij} – требуемый тип i-го ключа в j-ном разделе системного реестра; z_{ij} – требуемое значение i-го ключа в j-ном разделе системного реестра.

Формализованная модель процесса аудиторской проверки системного реестра для автоматического режима:

$$F_{aa}^{*} = F^{*} \cdot (X_{ij}), \mathrm{X}_{ij} \in V, \quad (7)$$

где

$$X_{ij} = (y_{ij}, k_{ij}, z_{ij}), \quad (8)$$

где X_{ij} – полученные параметры i-го ключа в j-ном разделе системного реестра; V – определенный набор ключей, предназначенный для автоматического режима работы программного комплекса; y_{ij} – полученное имя i-го ключа в j-ном разделе системного реестра; k_{ij} – полученный тип i-го ключа в j-ном разделе системного реестра; z_{ij} – полученное значение i-го ключа в j-ном разделе системного реестра.

В процессе аудиторской проверки происходит сравнение значений ключей требуемого состояния с полученными в ходе проверки данными.

Построение архитектуры на этапе разработки программы является неотъемлемой частью ее успешного функционирования. Ар-

Таблица 2

Сводная таблица популярного локального ВПО и его расположения в реестре

№	Название	Атакуемые пользователи, %	Расположение в системном реестре
1	Dangerousobject. Multi.Generic	23,1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Policies\System
2	Trojan.Win32. Generic	18,8	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Winlogon HKEY_USERS\DEFAULT\Software\Microsoft\ Windows\CurrentVersion\Internet Settings\ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\ Services\svflooje\Enum\
3	Trojan.Winlnk. Startpage.Gena	7,2	HKCU\Software\Microsoft\Internet Explorer\Main HKCU\Software\Microsoft\Internet Explorer\SearchURL
4	Trojan.Win32. Autorun.gen	4,8	HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\RunOnce
5	Worm.Vbs. Dinihou.r	4,6	HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKCR\WSFFile\Shell\Open\Command
6	Networm.Win32. Kido.ih	4,0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\SvcHost
7	Virus.Win32. Sality. Gen	4,0	HKEY_CURRENT_USER\Software\Microsoft\- Windows\CurrentVersion\Internet Settings HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\policies\system
8	Trojan.Script. generic	2,9	HKEY_LOCAL_MACHINE\SOFTWARE\Classes Ключи реестра, прописывающие работу браузера
9	Dangerouspattern. Multi.Generic	2,7	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Policies\System
10	Worm.Win32. Debris.a	2,6	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles

хитектура программного комплекса представлена на рисунке 1.

Архитектура разработанной программы состоит из следующих функциональных блоков:

а) пользовательский интерфейс;

б) ручной режим:

1) модуль запоминания значений ключей реестра – предназначен для сбора сведений о

Таблица 3

Сравнение внешнего ПО

Особенности	Программное обеспечение			
	RegShot	RegistryMonitor	RegistryAlert	RegFromApp
Страна-производитель	Китай	США	США	Англия
Процесс работы	Вручную	Вручную	Автоматический	Автоматический
Возможность выбора аудита отдельных разделов реестра	Да	Да	Нет	Нет
Автоматическое оповещение об обнаруженных изменениях в реестре	Нет	Да	Нет	Да
Способ создания эталонной модели	Снимок экрана	Снимок экрана	Не использует	Снимок экрана
Формирование отчета в HTML и текстовые форматы	Да	Нет	Нет	Да
Возможность хранения отчетов в базе данных	Нет	Нет	Нет	Нет
Демонстрация приложений обращающихся в реестр	Да	Да	Нет	Нет
Остановка процесса аудита при обнаружении проблем в реестре	Нет	Нет	Да	Нет
Язык интерфейса	Многоязычная поддержка	Английский	Английский	Многоязычная поддержка

Рис. 1. Архитектура программного комплекса аудита информационной безопасности по данным системного реестра на АРМ

системном реестре и создания эталонной модели состояния системного реестра;

2) модуль аудиторской проверки – предназначен для получения объективной и независимой оценки степени изменений состояния системного реестра и сравнения его с требуемым состоянием;

3) база данных ручного режима – предназначена для хранения отчетности о результатах проведения аудиторской проверки в ручном режиме;

в) автоматический режим:

1) модуль установки общих параметров – предназначен для ввода ключей, установки таймера и других функций;

2) модуль создания модели требуемого состояния – предназначен для сканирования и запоминания значений ключей системного реестра;

3) модуль аудиторской проверки – предназначен для получения объективной и независимой оценки степени изменений состояния системного реестра и сравнения его с требуемым состоянием;

4) модуль принятия решений – содействует оператору АРМ при выборе дальнейших действий после проведения аудиторской проверки;

5) база данных автоматического режима – предназначена для хранения отчетности о результатах проведения аудиторской проверки в автоматическом режиме.

В процессе систематической аудиторской проверки в автоматическом режиме пять раз в день в течение шестидневной рабочей недели программным комплексом RegWatcher была составлена статистика выявленных несоответствий требуемого состояния системного реестра с полученным. Данные представлены на рисунке 2.

В результате по итогам проведения аудиторской проверки с помощью разработанной программы было выявлено 15 изменений, 2 из которых являлись потенциально опасными для стабильной работы АРМ пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. Аудит информационных ресурсов // Information Security. – Электрон. текстовые дан. – Режим доступа: https://www.itsec.ru/articles2/Oborandteh/audit–informacionnyh–resursov. – Загл. с экрана.

	Понедельник	Вторник	Среда	Четверг	Пятница	Суббота
9.00	0	0	1	0	1	1
11.00	1	0	1	0	0	1
13.00	0	1	0	2	0	2
15.00	2	0	1	0	2	2
17.00	0	1	0	3	0	1

Рис. 2. Статистика выявленных несоответствий требуемого состояния системного реестра с полученным

2. Климов, А. Реестр Windows 7 / А. Климов. – СПб. : Питер, 2010. – 325 с.

3. Курило, А. П. Аудит информационной безопасности / А. П. Курило. – М. : БДЦ-Пресс, 2006. – 304 с.

4. Максимова, Е. А. Проблемы разработки частной политики менеджмента инцидентов информационной безопасности предприятия / Е. А. Максимова, Т. А. Омельченко, В. В. Алексеенко // Известия ЮФУ. Серия «Технические науки». – 2014. – Электрон. текстовые дан. – Режим доступа: http://izv-tn.tti.sfedu.ru/?p=9951, свободный. – Загл. с экрана.

REFERENCES

1. Audit informatsionnykh resursov [Audit of Information Resources]. *Information Security*. Available at: https://www.itsec.ru/articles2/Oborandteh/audit–informacionnyh–resursov.

2. Klimov A. *Reestr Windows 7* [The Registry of Windows 7]. Saint Petersburg, Piter Publ., 2010. 325 p.

3. Kurilo A.P. *Audit informatsionnoy bezopasnosti* [Information Security Audit]. Moscow, BDTs-Press Publ., 2006. 304 p.

4. Maksimova E.A., Omelchenko T.A., Alekseenko V.V. Problemy razrabotki chastnoy politiki menedzhmenta intsidentov informatsionnoy bezopasnosti predpriyatiya [Problems of Development of Private Policies of Management of Information Security Incidents at the Enterprise]. *Izvestiya YuFU. Seriya "Tekhnicheskie nauki"*, 2014. Available at: http://izv-tn.tti.sfedu.ru/?p=9951, svobodnyj.

AUDIT OF INFORMATION SECURITY OF THE USER'S COMPUTER WORKSTATION BASED ON SYSTEM REGISTRY DATA

Elena Aleksandrovna Maksimova

Candidate of Technical Sciences, Associate Professor,
Head of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Tatyana Aleksandrovna Omelchenko

Postgraduate Student, Researcher, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Yuriy Petrovich Umnitsyn

Associate Professor, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Kristina Petrovna Guzhakovskaya

Candidate of Physical and Mathematical Sciences, Associate Professor,
Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Information security audit is an independent assessment of the current state of information security, determinig the level of its compliance with certain criteria, and providing results in the form of recommendations.

There are many approaches to the maintenance of the required level of security of the computer workstation, while the approaches vary in the degree of their effectiveness and value characteristics. The use of traditional active and passive means of information protection in the enterprise is not always possible due to various reasons. One way out of this situation can be a continuous audit of the information system as a whole and its individual vital nodes.

An audit is an independent examination of the individual areas of functioning of the organization. There are two types of audit: external and internal. To protect your system registry from malicious attacks, it is necessary to control the undesirable activities that occur in the registry during the installation of each new program. To do it manually is impossible since the registry contains millions of records. It is therefore necessary to analyse the current external software tool designed to audit information security of the system registry on the workstation user.

The results of the audit with the help of the developed program identified 15 changes, 2 of which were potentially dangerous for the stable operation of the workstation user.

Key words: system registry, information security audit, computer workstation, information security, external attack.