СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2021. – № 1 (100).** – 64–79

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 519.24 DOI: 10.17212/2307-6879-2021-1-64-79

АВТОМАТИЗАЦИЯ ОБРАБОТКИ ДАННЫХ В ПРОЦЕССЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

В.Ю. ДРОНОВ[1], Г.А. ДРОНОВА[2], В.М. БЕЛОВ[3], Л.А. ГРИЩЕНКО[4], С.А. ЗЫРЯНОВ[5]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: dronov@corp.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: g.dronova@corp.nstu.ru*

[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доктор технических наук, профессор кафедры защиты информации. E-mail: v.m.belov@corp.nstu.ru*

[4] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: zyryanov@corp.nstu.ru*

[5] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: l.grishhenko@corp.nstu.ru*

Согласно российским стандартам в области менеджмента информационной безопасности (ИБ), являющимся аутентичными международным стандартам, таким как [1, 2], организация на регулярной основе должна осуществлять внутренний аудит системы менеджмента информационной безопасности. Аудит – это независимая проверка и оценка деятельности организации путем анализа и оценки процессов, проектов, отчетности, продуктов. Аудит, как вид деятельности, не является статичным, неизменным, он эволюционирует. С точки зрения ведущих международных аудиторских компаний, в частности [3, 4], современный этап эволюции аудита – это переход от реактивности (выявление недостатков постфактум) к проактивности (предсказательность результатов действий или событий до их завершения). Верность утверждения для российского внутреннего аудита подтверждена итогами IX Национальной научно-практической конфе-

* Статья получена 12 декабря 2020 г.

ренции [5]. Движение к проактивности в аудите определяет актуальность следующих задач:

1) обработка до 100 % информации, порождаемой деятельностью, находящейся в фокусе внимания аудита;

2) обработка информации в режиме, близком к онлайн;

3) наличие мощного инструментария для анализа данных и моделирования на их основе дальнейшего развития исследуемых событий, а также обладание соответствующими навыками работы с ним у аудиторов.

При проведении проверок у аудитора возникает дилемма. С одной стороны, он обязан предоставить владельцам / акционерам / руководству организации данные, максимально приближенные к достоверному состоянию процессов менеджмента ИБ, информацию о выявленных недостатках и рекомендациях по их устранению. С другой стороны, время проверки жестко ограничено; выгрузка исходных данных из информационных систем организации занимает значительное время; получаемые из различных информационных систем и других источников данные имеют различные, не всегда стандартные форматы; используемый инструментарий имеет недостатки, поскольку наиболее часто используемые в работе электронные таблицы (MSExcel, LOCalc) в силу внутренних ограничений уже не в состоянии обеспечить требуемый функционал.

Вышеприведенные, а также другие факторы, например: нежелание сотрудничать, скрытое противодействие персонала проверяемой организации, оценка работы аудиторов только по количественным показателям (количеству наблюдений или по времени, затраченному на одно наблюдение) – указывают на то, что проверки осуществляются поверхностно. При этом недостатки в процессах менеджмента ИБ могут быть обнаружены, однако объяснить их природу и дать действенные рекомендации бизнесу аудитору становится затруднительно.

Как результат, определенная в ГОСТ ИСО/МЭК 27002–2012 цель независимых проверок – «обеспечение уверенности в сохраняющейся работоспособности, адекватности и эффективности подхода организации к менеджменту информационной безопасности» [2] – не может быть достигнута.

Одним из вариантов устранения некоторых из вышеназванных недостатков является применение в ходе аудиторских проверок программ, разработанных самими аудиторами и предназначенных для оперативной обработки данных, – так называемая «малая автоматизация». Подобный подход, хотя и является низовым звеном в цепи автоматизации аудиторских процедур, тем не менее находится в рамках парадигмы развития аудита в направлении роботизации процедур и применения искусственного интеллекта, о чем говорится, например, в работах [3, 6, 7], а также подтверждается результатами конференций института внутренних аудиторов [8].

Ключевые слова: аудит, аудит информационной безопасности, информационная безопасность, автоматизация, Python

1. ОПИСАНИЕ ЗАДАЧИ

Современная система управления ИБ базируется на перечне организационно-технических требований ИБ, иногда называемых, например, «состав и содержание мер по обеспечению безопасности» (ОТТ). ОТТ для удобства обычно представляются в виде таблиц. В качестве иллюстрации можно привести соответствующие стандарты по ИБ-NISTSP 800-53 «Securityand Privacy Controls for Federal Information Systemsand Organizations» [10], а также ГОСТ Р 57580.1–2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [11], либо документы государственного регулятора в лице Федеральной службы по техническому и экспертному контролю: Приказ от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [12], Приказ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [13]. ОТТ организаций часто формируются в аналогичном виде.

В качестве примера приведем оценку степени выполнения одного из требований – «Защита от вредоносного кода» – некоей организации в его простейшем варианте: «на всех компьютерах должно быть установлено и функционировать актуальное антивирусное ПО» с помощью небольшой программы собственной разработки.

При стандартном подходе по запросу аудитора ИТ-служба должна предоставить актуальную информацию о составе компьютеров, ИБ-служба – актуальные отчеты АВПО. Сравнение перечней компьютеров в полученных от ИТ и ИБ данных иногда приводит к «странному» результату: они не совпадают! Если же дополнительно провести простейшее сканирование сети на предмет обнаружения активных хостов, например, с помощью команды ping, то можно получить еще более интересный результат: все три массива, назовем их SCCM, AV и Scan, не просто не совпадают, но и имеют значительные расхождения.

Инструментом «малой автоматизации» выбран язык программирования Python 3, являющийся очень простым для изучения, удобным для разработки и отладки ПО (особенно при использовании Jupyternotebook из пакета Anaconda), имеющий большое количество разработанных библиотек и пакетов по различным направлениям обработки информации и ее анализа. Кроме того, необходимо отметить его кросс-платформенность и возможность создавать исполняемые файлы для рабочих мест, не имеющие установленного Python.

2. РЕАЛИЗАЦИЯ

Программа «малой автоматизации» аудиторской процедуры оценки степени выполнения требования «Защита от вредоносного кода» помимо стандартных модулей загрузки библиотек, определения переменных и функций состоит из модулей подсказки, подготовки команд сканирования сети, обработки и сохранения результатов сканирования, анализа результатов.

Ниже приведено краткое описание отдельных модулей программы в виде поэтапного выполнения.

Этап 1. Подготовка данных для сканирования

Исходные данные представлены в виде файла электронных таблиц (MSExcel или LOCalc) и включают перечень подсетей, которые будут подвержены исследованию. В табл. 1 представлена часть перечня, выгруженная из SCCM. Для анализа достаточны только IP-адрес подсети и маска. С целью минимизации работы в качестве индикатора выбора подсети принято решение использовать цвет заголовка: аудитор устанавливает цвет шрифта заголовка, а затем помечает интересующие подсети тем же цветом.

Таблица 1

Перечень выбранных подсетей

Подсети IP	Маска IP-подсети
10.100.0.0	24
10.100.100.0	24
10.100.104.0	24
10.100.106.0	24
10.100.110.0	24
10.100.111.0	24
10.100.112.0	25
10.100.113.0	24

Этап 2. Запуск сканирования

При запуске программы производится загрузка библиотек, определение констант и функций. Поскольку программа универсальна для Linux и Windows, то на этапе загрузки определяются тип ОС и строки стандартных команд fping для них:

```
…
importos
importre# необходим для поиска цифр в строке
```

```
    import chardet                # работа с разными кодировками текста
    import ipaddress                              # работа с IP-адрессами
    …
    from sys import platform                    # определениетипаОС
    if platform == "linux" or platform == "linux2":
        workPath = "/root/Python/Pinger" # Linux
        OS = 'Linux'
    elif platform == "win32":
        workPath = "C:\\Python\\Pinger\\" # Windows
        OS = 'Windows'
    ……
    Cmd1 = "fping -Adegs "          # команда для Linux версии
    Cmd2 = "fping -A -n 1 -f -g " # команда для Windows версии
    …
    def ipCorrect(sIP, msk):   # обработка IP-адресов
        ipNet, ipSubNet, ipSSubNet, ipAdr = sIP.split('.')
        ipm = int(msk); ipl = 32 - ipm; ipcorr = 2**ipl
        ipn = int(ipAdr); ipn = ipn + ipcorr
        if ipn >= 255:
            ipn = 255
        iptext = ipNet + '.' + ipSubNet + '.' + ipSSubNet + '.' +
str(ipn)
    returniptext
```

Этап 3. Подсказка

Для информирования пользователя о работе с программой соответствующая информация собрана в отдельный файл и в случае необходимости выводится на экран в модуле подсказки. Сложность работы с подсказкой в необходимости определения кодировки файла подсказки для различных ОС:

```
    print('Нужна помощь (y)?')
    yes = input()
    if yes == 'y' or yes == 'Y':
        fnHlp = r'fping.help.txt'
        helphandle = open(fnHlp, 'rb')
        helpdata = helphandle.read()
        result = chardet.detect(helpdata)
        charenc = result['encoding']
        helphandle.close()

        helphandle = open(fnHlp, 'rt', encoding = charenc)
        for line in helphandle.readlines():
            print (line)
        helphandle.close()
```

Этап 4. Подготовка команд

Командный модуль предназначен для создания массива команд сканирования по выбранным подсетям. Каждая команда осуществляет вывод результатов в отдельный текстовый файл.

Команда формируется совокупностью одной из переменных – Cmd1 или Cmd2 (в зависимости от ОС) – и добавлением IP, соответствующего по цвету заголовку перечня подсетей, и его маски. Предварительно IP и маска проверяются на наличие ошибок (IP неправильного формата, маска не число или число вне пределов от 24 до 32). Перечень команд с параметрами размещается в списке netCtrl:

```
        # проверка формата маски
    msk = re.findall(r'\b\d+\b', str(ws.cell(x,2).value))
                maska = int(*msk);
                if maska <= 0 or maska > 32:
                    if maska < 24:
                        maska = 24
                 …
                # проверяем IP
                IP = str(ws.cell(x,1).value); IP2 = IP
                ipNum = int(ipaddress.ip_address(IP))
                try:
                    flag = True
                except:
                    flag = False # print("Неправильный IP")
    …
                # определяемся
                if flag == True:
                # имя файла для результата сканирования одной командой
    fileName = commandTime + "--" + IP + "@" + stMaska + ".txt"
                    if OS == 'Linux':
                        Command = Cmd1 + " " + IP + "/" + str(maska) + "
> " + fileName
                    elif OS == 'Windows':
                        IP2 = ipCorrect(IP, maska); Command = Cmd2 + " "
+ IP + "/" + IP2 + " -L " + fileName
                    else:
                        Command = Cmd1 + " " + IP + "/" + str(maska) + "
> " + fileName
                    netCtrl.append([[Count], [IP], [maska], [Command],
[fileName]])
```

Этап 5. Сканирование подсетей

Сканирование осуществляется путем запуска в виде shell-команд из перечня netCtrl, сформированного в предыдущем модуле. Сразу по завершении сканирования подсети и записи результатов в файл последний подвергается обработке на предмет определения откликнувшихся хостов. Результаты заносятся в список Host с последующей записью в файл электронной таблицы (табл. 2). Массив Scan сформирован:

```
# идем по командам
for i in range(Count):
cmdLine = str(netCtrl[i][3])
cmdLine = cmdLine[2:-2]
…
os.system(cmdLine)

# открыть txt-файл с fping'ами
with open(fileName) as txtF:
Host = []; IPv4 = []; Answ = []; Tim = []; Scan = []
for line in txtF:
 …
ifOS == 'Windows': # обработка результатов при ОС Windows
…
else: # Linux - обработка результатов при ОС Linux
…
Host.append(lstIP[0]); IPv4.append(lstIP[1]); Answ.append(lstIP[2]);
Tim.append(lstIP[3]); Scan.append(scanTime)
```

Таблица 2

Результаты сканирования в среде ОС Windows

Host	IP	Answer	Time
10.10.121.1	10.100.121.1	is alive	2.53 ms
10.10.121.6	10.100.121.6	is alive	2.25 ms
10.10.121.7	10.100.121.7	is alive	2.89 ms
10.10.121.12	10.100.121.12	is alive	3.71 ms
10.10.121.22	10.100.121.22	is alive	0.92 ms
10.10.121.23	10.100.121.23	is alive	19.7 ms
w-ia-0009.sib.local	10.100.121.27	is alive	6.40 ms
itc595.sib.local	10.100.121.31	is alive	1.63 ms

Окончание табл. 2

Host	IP	Answer	Time
10.10.121.41	10.100.121.41	is alive	0.62 ms
10.10.121.42	10.100.121.42	is alive	1.10 ms
10.10.121.49	10.100.121.49	is alive	0.85 ms
4515.sib.local	10.100.121.52	is alive	0.53 ms
2533.sib.local	10.100.121.57	is alive	0.66 ms
xrx9c934e182b8c	10.100.121.59	is alive	0.77 ms
10.10.121.60	10.100.121.60	is alive	3.43 ms
w-ia-0057.sib.local	10.100.121.67	is alive	0.70 ms
w-ia-0058.sib.local	10.100.121.68	is alive	0.78 ms
10.10.121.75	10.100.121.75	is alive	0.25 ms
i500.sib.local	10.100.121.81	is alive	0.57 ms
osvet1.sib.local	10.100.121.83	is alive	1.04 ms
10.10.121.253	10.100.121.253	is alive	0.25 ms
10.10.121.2	10.100.121.2	is unreachable	
10.10.121.3	10.100.121.3	is unreachable	
10.10.121.4	10.100.121.4	is unreachable	
10.10.121.5	10.100.121.5	is unreachable	

Этап 7. Сбор массивов

Сбор данных по контролируемым компьютерам (массив SCCM) и компьютерам, на которые распространено действие АВПО (массив AV), в единую электронную таблицу с массивом Scan необходим исключительно для удобства работы. Сбор осуществляется, например, средствами работы с файлами excel, в частности openpyxl, и трудности не представляет. Важно только обеспечить наличие обязательных столбцов, таких как IP, и соответствующее массиву состояние хоста (рис. 1–3).

Небольшую проблему представляет очистка массива Scan от хостов, не являющихся компьютерами (телекоммуникационные и периферийные устройства).

A	B	C	D	E	F	G	H	I	J	K	L	M	
№	IP	Имя компьютера	Подсеть	Посл. вход. пользователь	Домен	Операционная система	Пакеты обновлен	Серийный ном	Производитель	Модель	Память (Kbyte	Процессор	Проце
66	10.100.110.117	NE-EL-W-0767	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	P5KC	4193400	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz	
67	10.100.110.118	NE-EL-W-0768	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	System Product Name	4160656	Intel(R) Core(TM) i5-2310 CPU @ 2.90GHz	
68	10.100.110.119	NE-EL-W-0769	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Корпоративная	Service Pack 1		Hewlett-Packard	HP3520 Aio	3535388	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	
6	10.100.110.12	NE-EL-W-0570	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	System Product Name	4193336	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz	
69	10.100.110.120	NE-EL-W-0770	10.100.110.0		sibdomen.ru	Майкрософт Windows 10 Корпоративная			Hewlett-Packard	HP Pro 3420 AiO PC	4104660	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz	
70	10.100.110.121	NE-EL-W-0771	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Корпоративная	Service Pack 1		Hewlett-Packard	HP Pro 3500 Series	3551508	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	
71	10.100.110.122	NE-EL-W-0772	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	System Product Name	2087096	Pentium(R) Dual-Core CPU E5300 @ 2.60GHz	
72	10.100.110.123	NE-EL-W-0773	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	System Product Name	4193336	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz	
73	10.100.110.125	NE-EL-W-0774	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Default string	System manufacturer	System Product Name	8253392	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz	
74	10.100.110.126	NE-EL-W-0775	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	System Product Name	4160656	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz	
75	10.100.110.127	NE-EL-W-0776	10.100.110.0		sibdomen.ru	Майкрософт Windows 10 Pro		Default string	System manufacturer	System Product Name	8226044	Intel(R) Core(TM) i3-8100 CPU @ 3.60GHz	
76	10.100.110.128	NE-EL-W-0777	10.100.110.0		sibdomen.ru	Microsoft Windows 7 Профессиональная	Service Pack 1	Chassis Serial Number	System manufacturer	P5QL PRO	2096248	Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz	

Result | fPing | SCCM | AV

Рис. 1. Массив SCCM (обязательные столбцы – IP и имя компьютера)

A	B	C	D	E	F
№	IP	Имя компьютера	Базы давно не обновлялись	Агент администрирования не установлен или не работает	Не актуальная версия АВПО
1	10.100.110.103	NE-EL-W-0757			
2	10.100.110.104	NE-EL-W-0758	Y		Y
3	10.100.110.106	NE-EL-W-0759			
4	10.100.110.109	NE-EL-W-0761			
5	10.100.110.110	NE-EL-W-0762			
6	10.100.110.111	NE-EL-W-0763		Y	
7	10.100.110.112	NE-EL-W-0764	Y		
8	10.100.110.115	NE-EL-W-0765		Y	
9	10.100.110.116	NE-EL-W-0766			
10	10.100.110.117	NE-EL-W-0767			
11	10.100.110.118	NE-EL-W-0768			
12	10.100.110.119	NE-EL-W-0769			
13	10.100.110.12	NE-EL-W-0570	Y		
14	10.100.110.120	NE-EL-W-0770			
15	10.100.110.121	NE-EL-W-0771			
16	10.100.110.123	NE-EL-W-0773			
17	10.100.110.126	NE-EL-W-0775			
18	10.100.110.127	NE-EL-W-0776			
19	10.100.110.128	NE-EL-W-0777			
20	10.100.110.129	NE-EL-W-0778			
21	10.100.110.13	NE-EL-W-0595			
22	10.100.110.130	NE-EL-W-0779			

Result | fPing | SCCM | AV

Рис. 2. Массив AV (все столбцы обязательные, данные в столбцах D, E, F получены на этапе обработки исходных отчетов АВПО)

A	B	C	D	E	F
№	IP	Host	Answer	Time	ScanTime
1	10.100.110.1	10.100.110.1	is alive	21.7	21.7
2	10.100.110.10	10.100.110.10	request timed out		
3	10.100.110.100	10.100.110.100	request timed out		
4	10.100.110.101	10.100.110.101	request timed out		
5	10.100.110.102	10.100.110.102	request timed out		
6	10.100.110.103	10.100.110.103	is alive	0.7	0.7
7	10.100.110.104	10.100.110.104	is alive	2.0	2.0
8	10.100.110.105	10.100.110.105	request timed out		
9	10.100.110.106	10.100.110.106	is alive	0.8	0.8
10	10.100.110.107	10.100.110.107	request timed out		
11	10.100.110.108	10.100.110.108	is alive	2.9	2.9
12	10.100.110.109	10.100.110.109	is alive	0.8	0.8
13	10.100.110.11	10.100.110.11	request timed out		
14	10.100.110.110	10.100.110.110	is alive	0.5	0.5
15	10.100.110.111	10.100.110.111	is alive	1.2	1.2
16	10.100.110.112	10.100.110.112	is alive	0.9	0.9
17	10.100.110.113	10.100.110.113	request timed out		
18	10.100.110.114	10.100.110.114	request timed out		
19	10.100.110.115	10.100.110.115	is alive	0.8	0.8
20	10.100.110.116	10.100.110.116	is alive	0.6	0.6
21	10.100.110.117	10.100.110.117	is alive	0.7	0.7
22	10.100.110.118	10.100.110.118	is alive	7.5	7.5
23	10.100.110.119	10.100.110.119	is alive	0.8	0.8
24	10.100.110.12	10.100.110.12	is alive	21.5	21.5
25	10.100.110.120	10.100.110.120	is alive	1.0	1.0
26	10.100.110.121	10.100.110.121	is alive	0.6	0.6
27	10.100.110.122	10.100.110.122	is alive	0.5	0.5
28	10.100.110.123	10.100.110.123	is alive	0.9	0.9
29	10.100.110.124	10.100.110.124	request timed out		
30	10.100.110.125	10.100.110.125	is alive	0.7	0.7
31	10.100.110.126	10.100.110.126	is alive	0.7	0.7
32	10.100.110.127	10.100.110.127	is alive	0.6	0.6
33	10.100.110.128	10.100.110.128	is alive	0.7	0.7

Result | fPing | SCCM | AV

Рис. 3. Массив Scan (обязательные столбцы – IP, Host, Answer)

Этап 8. Анализ результатов

Этап также не представляет сложности. Можно делать как с использованием разработанных для целей аудита соответствующих модулей программы на Python, так и средствами электронных таблиц. Результат приведен на рис. 4.

A	B	C	D	E	F	G	H	I	J
№	Host	IP (1-254)	SCCM	AV	AV (нарушения)	is alive	Отклонение 1 (отклик отсутствующего в SCCM хоста)	Отклонение 2 (в отчетах АВПО отсутствуют хосты из SCCM или откликнувшиеся)	Отклонение 3 (все проблемы АВПО)
254	120	254	120	108	23	129	10	21	44
1	KNSMIR.sibdomen.ru	10.100.110.1	10.100.110.1			10.100.110.1		10.100.110.1	10.100.110.1
2	NE2438.sibdomen.ru	10.100.110.2	10.100.110.2	10.100.110.2		10.100.110.2			
3		10.100.110.3							
4	NE2612.sibdomen.ru	10.100.110.4	10.100.110.4	10.100.110.4		10.100.110.4			
5		10.100.110.5							
6	NE2747.sibdomen.ru	10.100.110.6	10.100.110.6	10.100.110.6		10.100.110.6			
7		10.100.110.7							
8	NE522.sibdomen.ru	10.100.110.8	10.100.110.8			10.100.110.8		10.100.110.8	10.100.110.8
9		10.100.110.9							
10		10.100.110.10							
11		10.100.110.11							
12	NE-EL-W-0570.sibdomen.ru	10.100.110.12	10.100.110.12	10.100.110.12	10.100.110.12	10.100.110.12			10.100.110.12
13	NE-EL-W-0595.sibdomen.ru	10.100.110.13	10.100.110.13	10.100.110.13					
14	NE-EL-W-0603.sibdomen.ru	10.100.110.14	10.100.110.14	10.100.110.14		10.100.110.14			
15		10.100.110.15		10.100.110.15		10.100.110.15	10.100.110.15		
16		10.100.110.16		10.100.110.16		10.100.110.16	10.100.110.16		
17		10.100.110.17							
18		10.100.110.18							
19	NE-EL-W-0606.sibdomen.ru	10.100.110.19	10.100.110.19	10.100.110.19	10.100.110.19	10.100.110.19			10.100.110.19
20		10.100.110.20							
21	NE-EL-W-0607.sibdomen.ru	10.100.110.21	10.100.110.21	10.100.110.21		10.100.110.21			
22	NE-EL-W-0608.sibdomen.ru	10.100.110.22	10.100.110.22	10.100.110.22		10.100.110.22			
23	NE-EL-W-0609.sibdomen.ru	10.100.110.23	10.100.110.23	10.100.110.23		10.100.110.23			
24		10.100.110.24							
25	NE-EL-W-0610.sibdomen.ru	10.100.110.25	10.100.110.25	10.100.110.25		10.100.110.25			
26	NE-EL-W-0611.sibdomen.ru	10.100.110.26	10.100.110.26	10.100.110.26	10.100.110.26	10.100.110.26			10.100.110.26
27	NE-EL-W-0612.sibdomen.ru	10.100.110.27	10.100.110.27			10.100.110.27		10.100.110.27	10.100.110.27
28	NE-EL-W-0614.sibdomen.ru	10.100.110.28	10.100.110.28	10.100.110.28		10.100.110.28			
29	NE-EL-W-0615.sibdomen.ru	10.100.110.29	10.100.110.29	10.100.110.29		10.100.110.29			

Result | fPing | SCCM | AV

Рис. 4. Результаты анализа состояния контроля «Защита от вредоносного кода»

РЕЗУЛЬТАТЫ И ВЫВОДЫ

Применение «малой автоматизации» в аудите ИБ позволяет следующее.

1. Сократить время на обработку информации операционного уровня.

Применение приведенной выше программы позволяет сократить время на получение результатов аудиторами ИБ.

Применение подобной автоматизации на втором уровне системы внутреннего контроля организации (в частности, в службе ИБ) с дополнением программы модулем автоматизированной выгрузки данных из SCCM и отчетов АВПО позволит в онлайн-режиме осуществлять контроль «Защиты от вредоносного кода» без применения дорогостоящих SIEM.

2. Получать более достоверные результаты.

Анализ результатов показал, что при традиционном подходе аудиторов происходит получение недостоверной оценки состояния защиты от вредоносного кода. Так, например, исходя из представленных отчетов (рис. 4) можно сделать вывод, что из 120 активных компьютеров только на 23 имеются проблемы с АВПО (19.2 %). Однако с учетом неконтролируемых SCCM хостов таких компьютеров 44 (37 %), что практически в два раза ухудшает предыдущий результат.

3. Включать в область проверки дополнительные контроли.

По результатам анализа получены три наблюдения вместо предполагаемых одного-двух. По плану оценки должны быть получены результаты о со-

стоянии контроля «Защита от вредоносного кода» в части наличия АВПО на всех компьютерах ОА и непосредственного наличия проблем с АВПО. Однако дополнительно получены данные о проблематичном состоянии «Контроль ИТ-инфраструктуры».

«Малая автоматизация» помогает эволюционному движению аудита ИБ в направлении достижения стратегической цели – «проактивности».

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: введ. 2008–02–01. – Переизд. – М.: Стандартинформ, 2019. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006 (дата обращения: 18.03.2021).

2. ГОСТ Р ИСО/МЭК 27002–2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности: взамен ГОСТ Р ИСО/МЭК 17799–2005: введ. 2014–01–01. – М.: Стандартинформ, 2014. – URL: http://docs.cntd.ru/document/1200103619 (дата обращения: 18.03.2021).

3. Ernst & Young. Does a disrupted Internal Audit (IA) function mean a stronger strategic partner? – 2018. – URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-future-of-internal-audit.pdf (дата обращения: 18.03.2021).

4. PricewaterhouseCoopers. Internal Audit Transformation: PwC. – 2020. – URL: https://www.pwc.com/us/en/services/risk-assurance/internal-audit-transformation.html (accessed: 18.03.2021).

5. Итоги IX Национальной научно-практической конференции «Внутренний контроль и аудит в России: Новые тенденции в условиях цифровизации». – М., 2020. – URL: http://nuiac.ru/ix-post (дата обращения: 18.03.2021).

6. *Chuprunov M.* Auditing and GRC Automation in SAP. – Berlin; Heidelberg: Springer, 2013. – 525 p.

7. Внутренний аудитор: журнал / издание Ассоциации «Институт внутренних аудиторов». – 2019. – № 1 (5). – 81 с.

8. NIST SP 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. – Rev. 4. – 2013. – 462 p. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (accessed: 18.03.2021).

9. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер: введ. 2018–01–01. – М.: Стандартинформ, 2020. –

179 с. – URL: http://docs.cntd.ru/document/1200146534 (дата обращения: 18.03.2021).

10. Приказ от 25.12.2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» / Федеральная служба по техническому и экспортному контролю. – М., 2017. – 32 с. – URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 18.03.2021).

11. Приказ от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» / Федеральная служба по техническому и экспортному контролю. – М., 2013. – 19 с. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения: 18.03.2021).

Дронов Вадим Юрьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: dronov@corp.nstu.ru

Дронова Галина Александровна, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: g.dronova@corp.nstu.ru

Белов Виктор Матвеевич, доктор технических наук, профессор кафедры защиты информации Новосибирского государственного технического университета. E-mail: v.m.belov@corp.nstu.ru

Грищенко Лев Аркадьевич, ассистент кафедры защиты информации Новосибирского государственного технического университета. E-mail: l.grishhenko@corp.nstu.ru

Зырянов Сергей Алексеевич, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. E-mail: zyryanov@corp.nstu.ru

DOI: 10.17212/2307-6879-2021-1-64-79

Automation of data processing in the process of information security audit*

V.Yu. Dronov[1], G.A. Dronova[2], V.M. Belov[3], L.A. Grishchenko[4], S.A. Zyryanov[5]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the information security department. E-mail: dronov@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the information security department. E-mail: g.dronova@corp.nstu.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, doctor of technical sciences, professor of the information security department. E-mail: g.dronova@corp.nstu.ru*
[4] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, postgraduate of the information security department. E-mail: l.grishhenko@corp.nstu.ru*
[5] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, candidate of technical sciences, associate professor of the information security department. E-mail: zyryanov@corp.nstu.ru*

According to the Russian standards in the field of information security management (IS), which are authentic international standards, such as [1, 2], the organization must regularly conduct an internal audit of the information security management system. An audit is an independent review and evaluation of an organization's activities by analyzing and evaluating processes, projects, reports, and products. Audit, as an activity, is not static, unchanging, it evolves. From the point of view of leading international audit companies, in particular [3, 4], the current stage of audit evolution is the transition from reactivity (identifying shortcomings after the fact) to proactivity (predicting the results of actions or events before their completion). The validity of the statement for the Russian Internal Audit is confirmed by the results of the IX National Scientific and Practical Conference [5]. The movement towards proactivity in the audit determines the relevance of the following tasks:

1) processing up to 100 % of the information generated by the activity that is the focus of the audit;
2) processing information in a close-to-online mode;
3) the availability of powerful tools for data analysis and modeling on their basis the further development of the investigated events, as well as the appropriate skills of working with it from the auditors.

When conducting audits, the auditors have a dilemma – on the one hand, they are obliged to provide the owners/shareholders/management of the organization with data as close as possible to the reliable state of the information security management processes, information about the identified shortcomings and recommendations for their elimination, on the other hand: the audit time is strictly limited; unloading the initial data from the organization's information systems takes considerable time; the data obtained from various information systems and other sources have different, not always standard formats; the tools used have disadvantages,

* *Received 12 December 2020.*

since the most frequently used spreadsheets (MSExcel, LOCalc), due to internal limitations, are no longer able to provide the required functionality.
The above-mentioned factors, as well as other factors, such as unwillingness to cooperate, hidden opposition of the personnel of the audited organization, evaluation of the work of auditors only by quantitative indicators (the number of observations or the time spent on one observation), lead to the fact that the checks are carried out superficially. At the same time, shortcomings in the information security management processes can be detected, but it becomes difficult to explain their nature and give effective recommendations to the business auditor.
As a result, the goal of independent audits defined in GOST ISO/IEC 27002-2012 – "ensuring confidence in the continued efficiency, adequacy and effectiveness of the organization's approach to information security management" [2] – cannot be achieved.
One of the options for eliminating some of the above-mentioned shortcomings is the use of programs developed by the auditors themselves and designed for operational data processing, the so-called "small automation", during audits. This approach, although it is a low-level link in the chain of automation of audit procedures and, nevertheless, is within the framework of the audit development paradigm in the direction of robotization of procedures and the use of artificial intelligence, which is discussed, for example, in the works [3, 6, 7], and also confirmed by the results of conferences of the Institute of Internal Auditors [8].

Keywords: audit, information security audit, information security, automation, Python

REFERENCES

1. GOST R ISO/MEK 27001–2006. *Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniya* [State standard R ISO/MEK 27001–2006. Information technology. Security techniques. Information security management systems. Requirements]. Moscow, Standartinform Publ., 2019. Available at: http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006 (accessed 18.03.2021).

2. GOST R ISO/MEK 27002–2012. *Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoi bezopasnosti* [State standard R ISO/MEK 27002–2012. Information technology. Security techniques. Code of practice for information security management]. Moscow, Standartinform Publ., 2014. Available at: http://docs.cntd.ru/document/1200103619 (accessed 18.03.2021).

3. Ernst & Young. *Does a disrupted Internal Audit (IA) function mean a stronger strategic partner?* 2018. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-future-of-internal-audit.pdf (accessed 18.03.2021).

4. PricewaterhouseCoopers. Internal Audit Transformation: PwC, 2020. Available at: https://www.pwc.com/us/en/services/risk-assurance/internal-audit-transformation.html (accessed 18.03.2021).

5. Itogi IX Natsional'noi nauchno-prakticheskoi konferentsii "Vnutrennii kontrol' i audit v Rossii: Novye tendentsii v usloviyakh tsifrovizatsii" [Results of

the IX National Scientific and Practical Conference " Internal Control and Audit in Russia: New trends in the context of digitalization»], Moscow, 2020. Available at: http://nuiac.ru/ix-post (accessed 18.03.2021).

6. Chuprunov M. *Auditing and GRC Automation in SAP*. Berlin, Heidelberg, Springer, 2013. 525 p.

7. *Vnutrennii auditor*, 2019, no. 1 (5). 81 p. (In Russian).

8. *NIST SP 800-53. Security and Privacy Controls for Federal Information Systems and Organizations*. Rev. 4. 2013. 462 p. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (accessed 18.03.2021).

9. GOST R 57580.1–2017. *Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer* [State standard R 57580.1–2017. Security of financial (banking) operations. Information protection of financial organizations. Basic set of organizational and technical measures]. Moscow, Standartinform Publ., 2017. Available at: http://docs.cntd.ru/document/1200146534 (accessed 18.03.2021).

10. Order of the FSTEC of Russia dated December 25, 2017, No. 239 "On approval of the requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation". (In Russian). Available at: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 18.03.2021).

11. Order of the FSTEC of Russia dated February 18, 2013 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems". (In Russian). Available at:https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (accessed 18.03.2021).

Для цитирования:

Автоматизация обработки данных в процессе аудита информационной безопасности / В.Ю. Дронов, Г.А. Дронова, В.М. Белов, Л.А. Грищенко, С.А. Зырянов // Сборник научных трудов. – 2021. – № 1 (100). – С. 64–79. – DOI: 10.17212/2307-6879-2021-1-64-79.

For citation:

Dronov V.Yu., Dronova G.A., Belov V.M., Grishchenko L.A., Zyryanov S.A. Avtomatizatsiya obrabotki dannykh v protsesse audita informatsionnoi bezopasnosti [Automation of data processing in the process of information security audit]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university*, 2021, no. 1 (100), pp. 64–79. DOI: 10.17212/2307-6879-2021-1-64-79.