8. Алимурадов А.К., Муртазов Ф.Ш. Методы повышения эффективности распознавания речевых сигналов в системах голосового управления. Измерительная техника. - 2015. - № 10. - С. 20 - 24.

9. Алимурадов А.К. Адаптивная компенсация помех речевых сигналов с использованием комплементарной множественной декомпозиция на эмпирические моды / А.К. Алимурадов // «Молодежь и XXI век - 2015»: материалы V Международной молодежной научной конференции (26-27 февраля 2015 года), в 3-х томах, Том 2, Юго-Зап. гос. ун-т., ЗАО «Университетская книга», Курск, 2015, С. 96 - 99.

М.Е. Бурлаков

ИССЛЕДОВАНИЕ ДИНАМИКИ АКТИВНОСТИ ПУБЛИКАЦИИ УГРОЗ В ОТКРЫТЫХ И ЗАКРЫТЫХ ИСТОЧНИКАХ ДАННЫХ

(Самарский национальный исследовательский университет им. С.П. Королёва)

Введение. В настоящее время остро стоит вопрос, связанный с обнаружением угроз и уязвимостей в области информационных технологий и программных комплексов. Более 87% пользователей компьютерных систем используют в качестве рабочей операционной системы - ОС *Windows* (в вариациях версий *Windows XP*, *Windows 7*, *Windows 8* и *Windows 10*) [1]. Исходя из этой статистики, злоумышленники не первый год уделяют повышенное внимание как данной операционной системе, так и программным решениям, функционирующих в рамках ОС Windows. Так, например, по данным компании *Hewlett Packard* [2] на сегодняшний день можно выделить более 500 классов различных уязвимостей в ПО.

К наиболее частым уязвимостям, по версии команды *TeamSHATTER*, в рамках информационных систем можно отнести [3]:

1. наличие специализированных логинов и паролей (пустые, по умолчанию, легко поддающиеся подбору);
2. SQL инъекции в различных реализациях взаимодействий с базами данных;
3. некорректно выданные права пользователя-исполнителя, ошибки в настройке привилегий групп;
4. слабое администрирование баз данных в части настройки необходимого функционала;
5. некорректная настройка разного рода конфигураций;
6. переполнение буфера (стека);
7. повышение привилегий;
8. атаки отказа в обслуживании (*DDoS*);
9. отсутствие своевременного обновление компонент безопасности баз данных;
10. хранение данных в отрытом (незащищенном виде).

Методы воздействия на ПО различны и причины появления могут быть как явными, так и неявными. Под явными ошибками есть следствие продуманных действий. Они сложно прогнозируемы с точки зрения каких-либо внешних систем. Зачастую результатом их появления служит мотивированные действия разработчика или группы разработчиков, направленных на целенаправленное ухудшение качества (в том числе и в области информационной безопасности) программного продукта. Прогнозирование и устранение явных ошибок во множестве случаев стоит начинать с работы с персоналом, то есть использованием социально-ориентированного подхода.

Неявные ошибки появляются по множеству причин, среди которых можно выделить следующие:

- невнимательность разработчиков ПО;
- некорректная организация тестирования ПО;
- отсутствие опыта;
- использованием ПО и библиотек с уже существующими угрозами и уязвимостями;
- небольшой горизонт видения развития программного продукта и т.д.

Неявные ошибки фиксируются как разработчиками ПО, так и злоумышленниками. Нередки ситуации, когда злоумышленники первыми обнаруживают угрозу и используют ее в качестве средства эскалации политик безопасности компьютерных систем.

Для публикации знаний об угрозах и уязвимостях злоумышленники используют как открытые, так и закрытые источники. Под закрытыми источниками понимаются источники, где доступ информации ограничен разного рода программно-аппаратными решениями. К таковым решениям можно, например, отнести:

- Процесс аутентификации, который можно разделить на:
  - базовую аутентификацию;
  - аутентификацию с подтверждением (*email*, телефона);
  - двухфакторную аутентификацию с привязкой к телефону;
  - иную вариацию аутентификации.
- Технологии:
  - *VPN, Proxy, Socks, Mesh, TOR* сети (подробнее можно узнать в [4-7]);
  - Доступ через канал связи с применением специальных сертификатов;
  - иные технологические ограничения.
- Другие решения, ограничивающие доступ к получению информации об угрозах и уязвимостях.

В случае, если доступ к информации не имеет никаких аппаратно-технических ограничений, источник называют открытым.

На открытых и закрытых источниках как злоумышленники, так и исследователи обмениваются информацией, становясь, таким образом, авторами об-

наруженных угроз и уязвимостей. Зачастую сигнализация о той или иной угрозе служит индикатором использования ПО для специалистов по компьютерной безопасности. В данной статье делается попытка исследовать авторов угроз и вывести из этого несколько выводов.

Анализ данных. В качестве исследования угроз были выбраны 10 наиболее часто скачиваемых программ для ОС *Windows* (по версии группы *Softonic*) [8] представленных в Таблице 1.

Таблица 1.ТОП-10 наиболее популярного ПО для работы в ОС Windows

№ п/п	Программа	№ п/п	Программа
1	*uTorrent*	6	*Whatsapp*
2	*SHAREit*	7	*Google Chrome*
3	*VLC media player*	8	*Adobe Reader*
4	*UC Browser*	9	*Adobe Flash Player*
5	*Mozilla Firefox*	10	*Internet Downloader Manager*

В качестве инструмента для исследования был взят комплекс *SCAN Project v.1.9.5* (далее *Scan*), разработанный в рамках НИОКР "Академия Инфотекс" . *Scan* выполняет следующие функции:

1. автоматизированный сбор информации об угрозах и уязвимостях программных комплексов;
2. выделение информации о времени появления угроз и уязвимостей;
3. выделение информации об авторах, заявивших об обнаружении.

В качестве анализируемого ПО было выбрано ПО из Таблицы 1 и уязвимости ОС *Windows* версий: *Windows XP*, *Windows 7*, *Windows 8* и *Windows 10*. Анализ данных проводился на информации полученной в промежутке времени с 1991 г. по настоящее время.

В качестве открытых и закрытых источников были взяты следующие источники (Таблица 2):

Таблица 2. Открытые и закрытые источники данных

Наименование источника	Ссылка	Тип
Security Lab	*http://www.securitylab.ru/*	Открытый
Exploit-DB	*https://www.exploit-db.com/*	Открытый
CVE Detail	*http://www.cvedetails.com/*	Открытый
Malwarebytes.org	*https://ru.malwarebytes.com/trial/*	Закрытый
Htbridge.com	*https:// htbridge.com*	Закрытый
web.nvd.nist.gov	*https://nvd.nist.gov/*	закрытый
0 day	*Onion TOR*	Закрытый
Seclists.org	*http://seclists.org/*	Закрытый
Stackoverflow	*Stackoverflow.com*	Открытый

Общее количество угроз на момент исследования ровнялось 269419. Общее количество уязвимостей, авторство у которых комплексу *Scan* не удалось обнаружить - 124049.

Общее количество авторов, заявивших об уязвимостях - 24975 (в среднем выходит по 5 угроз на каждого автора). Количество авторов заявивших хотя бы одну угрозу - 18704. Таким образом, можно сказать, что 75% всех угроз декларируются разными авторами (различие в плане логинов, под которым авторы оставляли информацию), что косвенно говорит о высокой персонификации данного рода исследований. Из этих расчетов следует что 6271 автор заявили о 105345 угрозах, в среднем по 16.7 на каждого. Таким образом 33.5% авторов ответственно за 84.9% заявленных угроз, что по логике соответствует принципу Парето. И тут можно говорить о системной работе т.е. вслед за найденной одной уязвимостью, авторы как правило обнаруживают еще несколько, с последующей публикацией в открытых и закрытых источниках.

В Таблице 3 представлены ТОП-10 наиболее активных авторов заявлявших об уязвимостях по представленным ПО.

Таблица 3.ТОП-10 авторов уязвимостей и угроз для программных продуктов

№ п/п	**Автор**	**Кол-во уяз-уяз-вимостей**	**Информация об авторе**	**Страна**
1	*CONFIRM*	16295	Под именем данного понимается множество производителей ПО, которые сами у себя обнаружили уязвимости и задекларировали их.	-
2	*BID*	10001	Некоммерческое сообщество специалистов в области информационной безопасности *SecurityFocus*, занимающееся поиском уязвимостей и угроз с дальнейшим декларированием разработчикам. Информация о группе http://www.securityfocus.com.	США
3	*XF*	9227	Группа специалистов IBM X-Force Research компании IBM, предоставляющих услуги в области информационной безопасности на коммерческой основе. Информация о группе http://www-03.ibm.com/security/xforce/	США
4	*MISC*	7864	Закрытое сообщество специалистов в области ИБ LEGAL HACKERS, занимающееся вопросами ИБ, "этическим" хакингом, тестированием на проникновение в ИС. Информация о группе http://legalhackers.com/	1.1 -
5	*BUGTRAQ*	5680	Список рассылок об уязвимостях именуемый Bugtraq Mailing List. Бесплатно предоставляющий информацию из своих источниках о найденных уязвимостях. Также занимается агрегацией информации из других источников. Информация о списке: http://seclists.org/bugtraq/	США
6	*VUPEN*	3445	Коммерческая структура, являющаяся ведущим поставщиком оборонных и наступательных технологий для разведки в области кибер-безопасности. Информация о структуре: http://vupen.com	США
7	*SECTRAC*	2848	Коммерческая структура *SecurityTracker*, являющаяся	США

	K		разработчиком ПО и поставщиком услуг в области ИБ (Vulnerability Notification Service). Информация о структуре: http://securitytracker.com/	
8	*MLIST*	1980	Открытое сообщество разработчиков ПО и специалистов в области ИБ *Openwall*. Информация о сообществе: http://www.openwall.com/	-
9	*MILW0RM*	1826	Крупное сообщество исследователей по безопасности (хакеров) . Агрегатор информации по другим источникам. Сайт сообщества: http://www.milw0rm.com/	-
10	*MS*	1567	Центр безопасности TechCenter компании Microsoft. Обособленное подразделение, созданное с целью исследования и обнаружения угроз, связанных с ОС Windows. Адрес центра: https://technet.microsoft.com	США

Таким образом, из 10 наиболее часто упоминаемых авторов 6 являются частными структурами с географическим расположением в США.

Одновременно с этим в таблице 4 представлены ТОП-10 наиболее активных авторов за последние 5 лет.

Таблица 4. ТОП-10 наиболее активных авторов за последние 5 лет

2012	**2013**	**2014**	**2015**	**2016**
CONFIRM(1493)	CONFIRM(1611)	CONFIRM(2082)	CONFIRM(2587)	CONFIRM(3210)
MISC(782)	MISC(429)	MISC(1665)	MISC(808)	MISC(390)
XF(531)	CISCO(330)	CERT-VN(765)	MS(425)	MS(365)
BID(490)	XF(300)	Ibm.com(598)	CISCO(400)	CISCO(268)
MLIST(340)	MLIST(213)	BID(594)	SECTRACK(262)	Google Security Research(213)
Metasploit(231)	SUSE(212)	XF(423)	APPLE(262)	MLIST(197)
Ordpress.org(175)	BID(206)	MLIST(328)	MLIST(259)	BID(159)
SECTRACK(174)	REDHAT(199)	SECTRACK(268)	Google Security Research(164)	APPLE(114)
OVAL(167)	Metasploit(193)	Cisco.com(223)	BID(158)	SUSE(105)
Drupal.org(134)	OVAL(193)	MS(207)	BUGTRAQ(140)	SECTRACK(101)

Исходя из этих данных, можно сказать, что только 4 сообщества поддерживают постоянную работу в области исследований уязвимостей и угроз: *CONFIRM*, *MISC*, *BID* и *MLIST*.

Выводы. Таким образом, исходя из имеющихся данных, можно заключить следующие выводы:

1. Количество обнаруженных угроз из года в год растет, что говорит о системных проблемах в разработке программного обеспечения и росте квалификации у злоумышленников

2. 6 из 10 сообществ, обнаруживших максимальное количество угроз за 2016 год – частные компании с географией США.

3. Количество разработчиков, не вовлеченных в сообщества по анализу уязвимостей велико, однако оно не оказывает решительного влияния на количество обнаруженных угроз.

4. Влияние открытых сообществ велико и количество обнаруженных и заявленных угроз постоянно растет.

5. Корпоративный сектор (Microsoft, IBM и др.) активно развивает направление в области информационной безопасности и аудита компьютерных сетей и программных комплексов.

Литература

1. W3Schools. OS Platform Statistics [Электронный ресурс]. – 2016. – Режим доступа: http://www.w3schools.com/browsers/browsers_os.asp

2. HP. The collateral damage of cybercrime [Электронный ресурс]. – 2016. –Режим доступа: http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

3. Trinidad Mark. Top 10 Database Vulnerabilities and Vulnerabilities and Misconfigurations [Электронный ресурс]. – 2012. – Режим доступа: http://www.sifma.org/uploadedfiles/societies/sifma_internal_auditors_society/top10-database-vulnerabilities-and-misconfigurations.pdf

4. *J. Applebaum* A Model of Outbound Client Traffic on The Tor Anonymity Network. // Wesleyan University. - 2013. - P. 54-58.

5. *Иванов М. А.* Криптографические методы защиты информации в компьютерных системах и сетях. // КУДИЦ-ОБРАЗ. - 2001. - С. 368-376.

6. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов // СПб.: Питер. - 2001. - 672 с..

7. *Столлингс В.* Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards //«Вильямс». - 2002. - С. 429-440.

8. Softonic. Top downloads [Электронный ресурс]. – 2016. – Режим доступа: http://en.softonic.com/windows/top-downloads

О.Н. Долинина, Н.К.Сучкова

ФОРМАЛЬНЫЕ МОДЕЛИ ОШИБОК КЛАССА «ИЗБЫТОЧНОСТЬ» В БАЗАХ ЗНАНИЙ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

(Саратовский государственный технический университет
имени Гагарина Ю.А.)

Введение

Интеллектуальные системы (ИС) принятия решений находят применение во множестве областей: промышленности, медицине, научно-исследовательской деятельности, образовании, что влечет за собой повышение требований к их надёжности. Особую роль при этом играет обеспечение качества баз знаний интеллектуальных систем, являющихся центральным звеном