Prospects of development the living creatures regeneration and immune mechanisms for the information security of computer systems
Turov V.
Перспективы использования иммунных и регенерационных механизмов живых существ для обеспечения информационной безопасности компьютерных систем
Туров В. Н.

Туров Владимир Николаевич / Turov Vladimir – дипломированный специалист,
факультет информационной безопасности,
Институт криптографии связи и информатики
Академия Федеральной Службы Безопасности Российской Федерации, г. Москва

Аннотация: *в статье анализируются ранее предложенные биоинспирированные механизмы обеспечения информационной безопасности компьютерных систем и перспективы их развития.*
Abstract: *the article analyzes existing bio-inspired mechanizms for information security computer system and prospects of development for this idea.*

Ключевые слова: *искусственные иммунные системы, биоинспирированные механизмы защиты компьютерных систем.*
Keywords: *artificial immune system, bioinspired defense mechanisms for computer systems.*

В настоящее время компьютерные системы применяются повсеместно, различные виды и типы устройств, используемых нами каждый день, такие как телевизоры, планшеты, мобильные телефоны, камеры, терминалы оплаты, системы допуска в помещения, а в последнее время и другие устройства вплоть до утюгов, представляют собой вполне самодостаточные компьютеры. Большинство из этих устройств подключены к глобальной сети Интернет и предоставляют нам больше комфорта, позволяя управлять своим «умным домом» прямо со своего, не менее «умного» мобильного телефона. Подключение к глобальной сети даёт устройствам возможность получать наши команды, обмениваться сообщениями друг с другом, загружать новые данные об окружающей среде, используемые в их работе, а также автоматически обновлять своё программное обеспечение в соответствии с новыми стандартами, законодательным актам и т.д., позволяя нам всё меньше заботиться о поддержке ПО устройств в актуальном состоянии. Более того, часто мы даже забываем, что в нашем телевизоре существует самостоятельный компьютер с выходом в Интернет, способный на достаточно мощные вычисления, и обладающий потенциалом как использовать собственные ресурсы (как, например, встроенные камеру и микрофон), так и ресурсы других систем по сети. Каждое из таких устройств работает под управлением некоторой операционной системы, использует определённое программное обеспечение, но в целом намечается заметная тенденция к унификации интерфейсов и используемого ПО таких мини- и микро-компьютеров. Унификация интерфейсов и стандартизация ПО ведёт не только к качественному его улучшению и облегчению взаимодействия устройств, но и к росту привлекательности использования уязвимостей такого ПО для злоумышленников.

Таблица 1. Количество устройств с выходом в интернет с прогнозом до 2020 года [1]

Показатель\Год	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Всего устройств (млрд шт.)	1450	1500	1550	1600	1650	1700	1750	1800	1850
Процент подключённых (%)	0,60	0,75	0,93	1,14	1,39	1,67	1,99	2,34	2,71
Устройств он-лайн (млрд шт.)	8,70	11,20	14,40	18,20	22,90	28,40	34,80	42,10	50,10

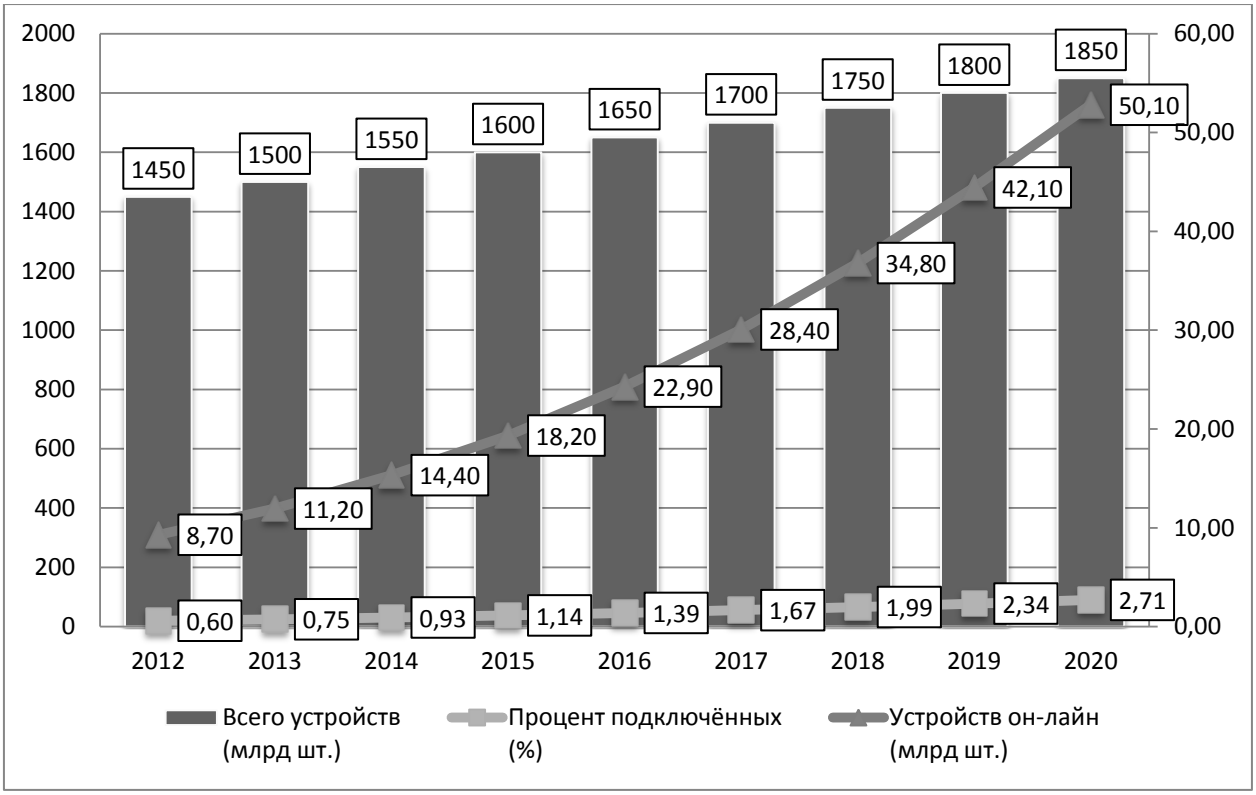

Рис. 1. Количество устройств с выходом в Интернет

В связи с масштабами компьютеризации всей окружающей нас инфраструктуры сложно переоценить влияние компьютерных систем на любую из сфер жизни сегодняшнего общества, поэтому сама проблема защиты компьютерных систем явно вышла на передний план, причём вышла далеко вперёд остальных. Даже некорректное поведение системы управления домашним утюгом теоретически может вызвать масштабный пожар, поэтому очевидно, процессы крупного производства и ключевые сферы безопасности, которые уже давно находятся под контролем специализированных компьютерных систем, требуют ещё более пристального внимания. Существующие на сегодняшний день средства защиты предлагают лишь частичные решения для определённых изученных ранее угроз, требуя от пользователей таких средств дополнительных финансовых и временных затрат на поддержание приемлемого уровня защиты. Например, защита от вредоносного ПО в большинстве случаев реализуется за счёт использования специального антивирусного ПО, осуществляющего проверку компонентов компьютерной системы на наличие изученных ранее сигнатур вредоносного ПО. Базы сигнатур обновляются производителем антивирусного ПО и поставляются пользователям, осуществившим подписку. В большинстве случаев подписка на получение обновлений антивирусного ПО является платной, так как требует от производителей такого ПО затрат на поиск и извлечение сигнатур всё новых и новых вредоносных программ, появляющихся каждый день. Но даже частые обновления баз не могут полностью обезопасить систему при встрече с новым вредоносным ПО, не проанализированным ранее производителем антивирусного ПО.

Таблица 2. Эффективность антивирусов по данным COMSS [2]

Антивирусные программы	Обнаружение	Вебзащита	Самозащита	Ложные
Qihoo 360 Internet Security 2014	98,10	100,00	50,00	3
BullGuard Internet Security 2014	97,00	100,00	100,00	0
Kaspersky Internet Security 2014	92,40	86,70	100,00	0
G Data InternetSecurity 2014	98,00	100,00	50,00	1
Emsisoft Internet Security Pack 8	97,30	73,30	50,00	0
F-Secure Internet Security 2014	97,10	93,30	50,00	0

Bitdefender Antivirus Free Edition	96,70	100,00	50,00	0
McAfee Internet Security 2014	98,20	73,30	100,00	2
Norton Internet Security 2014	96,20	73,30	100,00	1
Bitdefender Internet Security 2014	96,60	100,00	0,00	0
avast! Internet Security 2014	91,90	80,00	100,00	0
TrustPort Internet Security 2014	98,10	60,00	0,00	0
Ad-Aware PRO Security 11	96,10	93,30	0,00	0
Avira Internet Security Suite 2014	96,10	46,70	50,00	1
Comodo Internet Security Premium 6.3	90,80	20,00	50,00	4
ESET NOD32 Smart Security 7	95,20	86,70	50,00	0
Avira Free Antivirus 2014	96,10	26,70	50,00	0
Ashampoo Anti-Virus 2014	97,20	66,70	0,00	1
Trend Micro Titanium Internet Security	92,60	100,00	0,00	2
IObit Advanced SystemCare Ultimate	97,10	40,00	50,00	2
Panda Cloud Antivirus PRO 2.3	96,10	6,70	50,00	0
Panda Internet Security 2014	96,70	13,30	0,00	0
eScan Internet Security Suite	97,60	40,00	50,00	0
Microsoft Windows Defender 4.3	72,10	86,70	100,00	0
Outpost Security Suite PRO 9.0	93,70	20,00	50,00	0
Avast! Antivirus Free 2014	91,90	66,70	100,00	0
Ad-Aware Free Antivirus+ 11	96,20	13,30	0,00	0
ZoneAlarm Free Antivirus + Firewall	90,70	86,70	50,00	0
Norman Security Suite PRO 10	96,40	46,70	0,00	0
AVG Internet Security 2014	91,20	60,00	100,00	0
ZoneAlarm Internet Security Suite	90,80	80,00	50,00	0
AVG Anti-Virus Free 2014	91,20	46,70	100,00	1
Quick Heal Internet Security 2014	68,00	66,70	50,00	1
Webroot SecureAnywhere AntiVirus 14	58,70	73,30	100,00	8
Dr.Web Security Space 9	94,70	33,30	50,00	0

Обнаружение - общий уровень обнаружения антивируса (количество обнаруженных угроз) в процентах при проверке 3039 вредоносных файлов.

Веб-защита - процент заблокированных фишинговых и вредоносных веб-сайтов. Использовался набор из 10 фишинговых и 5 вредоносных веб-сайтов.

Самозащита - уровень самозащиты антивируса при проверке с помощью Process Hacker выгрузки основных работающих в системе процессов антивирусной защиты с последующим контролем защитных возможностей.

Ложные - количество ложных срабатываний при проверке 855 709 чистых файлов после установки 150 программ в систему.

Более того, антивирусные системы не имеют возможности определить некорректное поведение стандартного ПО, спровоцированного программными ошибками, которое также потенциально может нанести вред программной или даже аппаратной части компьютерных систем (далее – КС).

Таким образом, в связи с возрастающим масштабом применения компьютерных систем и, соответственно, потенциала по их использованию в ненадлежащих целях, а также в связи с унификацией используемого ПО и, соответственно, возможностей по использованию его уязвимостей, возрастает количество и специфичность вредоносного ПО. С другой стороны, используемые в настоящее время методы

борьбы с вредоносным ПО не способны защитить компьютерные системы от угроз, не встречавшихся ранее или не являющихся намеренно созданными.

На взгляд автора, большинство технологий и методов, использующихся в компьютерных системах, тем или иным образом были изначально заимствованы из механизмов, подсмотренных человеком в живой природе. Стоит отметить, что многие из этих механизмов также являются прямым отражением механизмов организации человеческого общества. Те же вредоносные программы, по сути, являются аналогами вирусов, от которых и получили своё общепринятое название, их аналогом в человеческом обществе является преступный образ жизни отдельных личностей или их групп, пытающихся через различные виды воздействия воспользоваться ресурсами и благами других людей и сообществ. Естественно, природные механизмы весьма сложны за счёт неоднородности живой природы и, зачастую, до сих пор до конца не изучены, их «аналоги» в общественной и информационной сферах гораздо примитивнее. Поэтому для рассмотрения и использования сути природных механизмов не требуется их абсолютное осознание, достаточно близкой модели. В частности, важно рассмотреть защитные механизмы, которые живые организмы применяют для поддержания жизни в конкурентных и агрессивных условиях окружающей среды. Ведь многообразие живых организмов порождает ситуацию с растущим потенциалом для использования и соответствующим ростом числа хищников и паразитов, стремящихся использовать существующие ресурсы других живых организмов с целью минимизации затрат собственных ресурсов. В таких жёстких условиях живые организмы были вынуждены найти лучшие из возможных способов защиты на всех уровнях жизнедеятельности. К примеру, механизмы иммунитета, созданные в процессе эволюции, позволяют уничтожать инородные объекты внутри организма, а также части самого организма, утратившие возможность функционировать корректно по тем или иным причинам. При этом практически все живые организмы имеют возможности обнаружения вредных воздействий и регенерации при необратимых повреждениях части организма, позволяя частично или полностью восстановить его функциональность, восстановив или заменив разрушенные ткани. Рассматривая механизмы иммунитета можно заметить, что существует чёткая специализация иммунных клеток – некоторые из них являются агентами, позволяющими обнаружить место проявления проблемы, другие блокируют повреждённые участки, позволяя локализовать последствия, отдельные клетки специализируются на выявлении и маркировке инородных объектов, нестандартно функционирующих собственных клеток, существуют специализированные уничтожители маркированных объектов, а также очищающие клетки, удаляющие последствия уничтожения инородных объектов и т.д. Каждый из этих механизмов, с точки зрения автора, было бы полезно рассмотреть в качестве механизма защиты компьютерной системы.

В настоящее время в России исследованию аспектов использования биоинсперированных механизмов защиты КС посвящен ряд работ, подавляющее большинство из которых посвящено использованию лишь иммунного механизма, основанного на анализе временных срезов состояний системы либо анализу событий системы (активного аудита). Многие из них послужили основополагающими источниками при проведении данного исследования. В частности, автор опирался на труды таких отечественных ученых как: Кашаев Т. Р., Оладько А. Ю., Котов В.Д., Васильев В. И. Нестерук Ф. Г., Осовецкий Л. Г., Нестерук Г. Ф., Воскресенский С. И. Котенко, И. В., Кондратьев А. А., Талалаев А. А., Тищенко И. П., Фраленко В. П. и других.

Наряду с отечественными работами автор обращался к трудам зарубежных специалистов, в той или иной степени касавшихся теоретических и практических вопросов биоинспирированных методов защиты КС: Халл Ж. М., Фринке Д. А., Харт Е., Тиммис Ж., Хофмейр С. А., Форрест С. И. и других.

В работах этих ученых рассматриваются вопросы создания методов определения инородности объектов КС по отношению к её нормальному состоянию, обучения системы, анализа эффективности таких систем для защиты от определённого типа атак, а также ряд других научных и практических обобщений, составляющих теоретическую и методологическую базу настоящего исследования. Однако тема создания полного метода защиты КС, использующего другие механизмы иммунного ответа и естественные механизмы регенерации, несмотря на ее очевидную научно-практическую актуальность и значимость, объектом отдельного исследования еще не выступала.

В работе [3] предлагается подход анализа нормального поведения пользователей и процессов системы на основе генерации множества «детекторов» - векторов, описывающих некорректное поведение системы для попытки определить некорректное поведение за счёт совпадения одного из таких «детекторов» с текущим вектором характеристик системы. На взгляд автора, существенным недостатком данного подхода является необходимость изначально собрать полный набор всех возможных векторов, описывающих нормальное поведение системы для каждого пользователя системы, это очевидно не является простой задачей, особенно с учётом постепенного роста функционала, используемого пользователем. Данный подход также не способен решить большинство задач, связанных с обеспечением безопасности КС на начальном этапе (когда

производится сбор информации о действиях пользователя и соответствующих срезах характеристик системы).

В работе [4] представлено более комплексное предложение модели иммунной системы КС, созданной в соответствие иммунной системе живого организма, но в данной работе также используется предположение о построении «вектора совместимости поведения», который должен описать все варианты нормальной активности системы. В данной работе не учитывается конкретика предполагаемых атак и объектов мониторинга, что, с одной стороны, позволяет описать процесс в целом на достаточно высоком уровне, но, с другой стороны, снижает практическую значимость полученных результатов. Автору представляется, что для облегчения получения результатов в разрезе защиты КС необходимо вначале сфокусироваться на защите от угроз определённого рода, например, целостности информации (что является целью подавляющего большинства атак на ИС) и несанкционированного доступа.

Например, в работе [5] искусственные иммунные системы в КС были рассмотрены с целью решения задачи обеспечения безопасности сетевого взаимодействия КС.

Практически во всех работах, связанных с иммунными системами предлагается анализировать состояние системы во временных срезах в качестве критерия нормального состояния. Лишь в некоторых работах [7] делаются более существенные предположения о конкретных характеристиках, которые можно было бы использовать в качестве основного критерия безопасности информационной системы. Проблема состоит в том, что описание состояния всей системы в целом – весьма трудоёмкая задача, тем более сложной является задача сопоставления текущего состояния системы с набором «детекторов», поэтому необходимо разработать метод определения состояний составляющих элементов информационной системы, с которыми уже можно было бы работать для реального анализа корректности поведения. Также важным вопросом, нуждающимся в полноценной проработке, является набор возможных действий, которые информационная система может противопоставить атакующим действиям нарушителя. В большинстве работ эти действия описываются на очень высоком уровне без конкретизации.

Таким образом, необходимость разработки системного подхода и создание рекомендаций по совершенствованию методов защиты КС на основе природных иммунных и регенерационных механизмов живых существ, актуальны для дальнейшего исследования.

Литература

1. Исследование компании Cisco о количестве используемых устройств с выходом в Интернет по годам. URL: http://blogs.cisco.com/news/cisco-connections-counter/ (дата обращения: 31.07.2016).
2. Исследование эффективности антивирусов. URL: http://www.comss.ru/page.php?id=2000/ (дата обращения: 30.07.2016).
3. *Кашаев Т. Р.* Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем, 2008. Кандидат технических наук. Уфа. 05.13.19 131 с.
4. *Оладько А. Ю.* Модель адаптивной многоагентной системы защиты в ОС Solaris 10 // Известия ЮФУ. Технические науки, 2011. № 12 (125). С. 210-217.
5. *Котов В. Д., Васильев В. И.* Система обнаружения сетевых вторжений на основе механизмов иммунной модели // Известия ЮФУ. Технические науки, 2011. № 12 (125). С. 180-190.
6. *Нестерук Ф. Г., Осовецкий Л. Г., Нестерук Г. Ф., Воскресенский С. И.* К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы, 2004. № 4. С. 25-31.
7. *Andreas Pietzowski, Benjamin Satzger, Wolfgang Trumler, Theo Ungerer.* A Bio-Inspired Approach for Self-Protecting an Organic Middleware with Artificial Antibodies /// Universität Augsburg. URL: https://www.informatik.uni-augsburg.de/de/lehrstuehle/sik/publikationen/papers/2006_iwsos_pie/iwsos2006.pdf./ (дата обращения: 31.07.2016)