Windows 2000, Windows XP, Windows Vista, Windows 7, Windows CE, Windows Mobile, Windows Embedded и др.). Почти столько же версий существует и *современных* ОС.

У компании Apple в портфеле также имеются сотни операционных систем: A/UX, Apple Darwin, Apple DOS, GS/OS, Mac OS, Mac OS8, Mac OS9, Mac OSX (от версии 10.0 Cheetah до 10.7 Lion), IOS, ProDOS, SOS. Наиболее широко используемые устаревшие ОС компании IBM: IBSYS, OS/2 (более 20 версий), AIX, DYNIX, OS/400, PCDOS и др.

Если говорить только об одном из мировых лидеров по разработке операционных систем Microsoft, то следует напомнить ряд общеизвестных фактов, ускоривших исследования в области ОС с иммунитетом.

Еще в далеком 2002 г. Билл Гейтс написал сотрудникам «Microsoft» известное письмо-рекомендацию о том, что «нужно исправлять ситуацию и пора начинать разрабатывать ПО с учетом требований безопасности». Эта инициатива затем получила название «Trustworthy computing» и до сих пор «развивается» – так появились windows vista, OSX и другие, в которых уже были заложены специальные механизмы, затрудняющие (но не исключающие) эксплуатацию уязвимостей.

Написать эксплойт для уязвимости в системе, в которой внедрены механизмы вроде вышерассмотренных DEP и ASLR, стало значительно сложнее.

Тем не менее в 2004 г. компания «Microsoft» заявила о краже 600 млн байт, 31 тысячи файлов и 13,5 млн строк исходного кода ОС Windows 2000 и Windows NT4. Преступников найти так и не удалось.

В 2017 г. произошла, как тогда считалось, – самая массовая кибератака в истории – вирус Wana Cryptir 2.0 заразил десятки тысяч компьютеров по всему миру. В блоге Kaspersky Lab тогда уточнялось, что Wana Cryptir 2.0 – это версия Wana Cry, использующая уязвимость под названием Ethernalblue, подробно описанная в выложенных документах хакерской группировки Shadowbrokers, взломавшей файлы АНБ.

Еще факт – разработанное хакерами вредоносное ПО под кодом HDD Cryptor не дает возможности компьютерам с ОС Windows даже загрузить операционную систему.

Распространялся этот червь-шифровальщик через использование очередной, выявленной хакерами, уязвимости в ОС. В общей сложности тогда вирус заразил более 200 тысяч компьютеров в 150 странах мира, нанеся при этом большой финансовый ущерб.

Недавний пример – в июле 2020 г. компания Microsoft пообещала исправить критическую ошибку безопасности новых версий Windows. Об этом сообщает издание ZDNet со ссылкой на отчет компании.

Американская корпорация официально признала ошибку и заявила, что исправляющие ее патчи будут доступны в следующем обновлении ОС. До его выхода специалисты компании рекомендовали пользователям перезагружать систему при появлении сообщений об ошибке.

На очередные проблемы с безопасностью Windows 10 в июле 2020 г. обратили внимание многочисленные пользователи операционной системы. Владельцы лицензионных копий ОС жаловались, что часто получали ошибки при попытке запустить приложения «песочницы» (Windows Sandbox) и «Защитника Windows»

(Windows Defender). С этой проблемой столкнулись пользователи Windows 10 версий 1903, 1909 и 2004.

Как известно, «песочница» необходима для обеспечения безопасного запуска потенциально опасных приложений без нанесения вреда системе. Программа является широко востребованной среди IT-специалистов.

Ранее источники сообщили, что Microsoft изменит порядок обновления своих операционных систем. Компания планирует ежегодно выпускать глобальные патчи для Windows 10X весной, для Windows 10 – осенью.

Почему вообще становятся возможными столь масштабные кибератаки? Ответ заключается в архитектуре современных информационных систем, которая основана на фундаментальном теоретическом базисе 70-х годов прошлого века. Именно тогда создавались первые ОС и ***проблемы массовых кибератак тогда фактически не существовало***. Конечно, современные коммерческие ОС защищены во много раз лучше, но ведь основные принципы их построения фактически не очень сильно изменились за прошедшее время.

В одном из интервью на эту тему Евгений Касперский заявил: «Абсолютно защищенных IT-систем не существует. Поэтому здесь необходим такой уровень защиты, при котором стоимость разработки атаки на компанию или пользователя превысит сумму возможного ущерба. Я называю этот принцип ***«кибериммунитетом»***. Он должен прийти на смену принципу «кибербезопасность». Безопасность должна лежать в основе каждой ИТ-системы, а не быть надстройкой над ней, как это происходит сейчас. В таком случае есть шанс сделать стоимость атаки настолько дорогой, что ее реализация будет просто бессмысленной. Это и будет основой безопасного цифрового мира».

Следует здесь отметить, что большинство экспертов по кибербезопасности в термин «кибериммунитет» вкладывают несколько иной смысл, о чем мы поговорим дальше.

4.3.2. Цифровые иммунные системы как перспективный инструмент сетевой защиты

Как мы видим, в настоящее время большинство информационных технологий (ИТ) и ИТ-систем создаются без учета воздействия на них «неблагоприятных факторов» – незадекларированных возможностей программно-аппаратных средств, вирусов, хакерских атак и др. Именно по этой причине для надежного (безопасного) функционирования в реальной среде такие ИТ-системы и приходится дооснащать дорогостоящими инструментами – сетевыми экранами, антивирусными программами и другими средствами защиты.

Кроме неизбежного усложнения архитектуры ИТ-системы это всегда оставляет вероятность уязвимости к внешним хакерским атакам, поскольку *преодолев эти защитные барьеры, высококвалифицированный злоумышленник попадает в незащищенное пространство операционной системы (ОС), где можно выполнять свои «негативные действия»*.

Как известно, человек нередко создает новые технологии, которые работают по тем же общим принципам, что и отдельные органы биологического объекта –

человека, животного, насекомого и т.д. Примеры – нейронные сети, искусственный интеллект, искусственная сетчатка глаза, алгоритмические средства обработки видеоизображений (зрительных образов) и многое другое.

Прежде чем кратко рассмотреть перспективное направление «искусственные иммунные системы» (AIS – Artificial Immune System), напомним, каким же образом функционирует иммунная система человека. Причем описание это будет очень упрощенным, с целью лишь обозначить те основные «биологические» элементы, которые переносятся в «компьютерные» сети.

Главным принципом действия человеческой иммунной системы является сравнение определенных «шаблонов» с находящимися внутри организма телами и выявление таким образом инородных тел, называемых антигенами (https://itc.ua/articles/iskusstvennye_immunnye_sistemy_kak_sredstvo_setevoj_samozashhity_4270/).

Роль подобных шаблонов у человека выполняют лимфоциты, постоянно генерируемые спинным мозгом и тимусом с учетом информации, содержащейся в ДНК (такая информация все время накапливается, и процесс этот называется *эволюцией генной библиотеки*), и разносимые организмом через лимфатические узлы, причем каждый тип лимфоцита отвечает за обнаружение какого-то ограниченного числа антигенов. При генерировании лимфоцитов имеется одна очень важная стадия, называемая *негативной селекцией*, на которой происходит своеобразный тест на соответствие «родным» клеткам организма: если подобное соответствие имеет место, «зародышевый» лимфоцит убивается, ведь в противном случае он будет бороться с собственными клетками. Иными словами, благодаря негативной селекции создаются «шаблоны», содержащие ту информацию, которая внутри организма отсутствует, и если какое-то тело подходит под данный шаблон, значит, оно явно чужое.

В случае обнаружения лимфоцитами антигена на основании соответствующего шаблона у человека вырабатываются антитела, которые и уничтожают его. Здесь задействуется еще один процесс – *клональная селекция*, во время которой происходит своеобразный естественный отбор антител: выживают лишь те, что максимально подходят под найденный антиген. При этом сведения о сгенерированных антителах «заносятся» в упоминавшуюся выше «генную библиотеку» (https://itc.ua/articles/iskusstvennye_immunnye_sistemy_kak_sredstvo_setevoj_samozashhity_4270/).

Специалистами, работающими сегодня в области AIS, отмечаются три основных свойства иммунной системы человека: во-первых, она является *распределенной*; во-вторых, она *самоорганизующаяся*; и в-третьих, она относительно «*легковесна*», или, говоря на «информационном» языке, не особо требовательна к вычислительным ресурсам. Именно этими свойствами, по мнению многих экспертов, должна обладать система обнаружения вторжений в информационную сеть (IDS – Intrusion Detection System).

IDS для одного сегмента цифровой сети, построенная на принципах искусственной иммунной системы, подразделяется на «основную» и набор «вторичных». Основная является неким аналогом спинного мозга, а вторичные – аналогами лимфатических узлов.

Как показано на рис. 4.1 (https://itc.ua/articles/iskusstvennye_immunnye_sistemy_kak_sredstvo_setevoj_samozashhity_4270/), в основной IDS на базе AIS имитируются два процесса – эволюция «генной библиотеки» и негативная селекция.

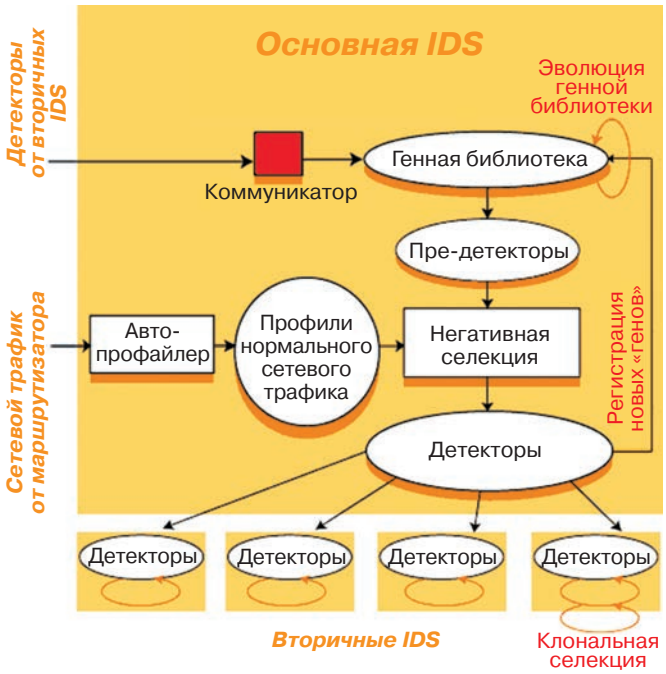

Рис. 4.1. Концепция построения IDS на принципах искусственной иммунной системы

На этапе эволюции генной библиотеки происходит накопление информации о характере аномалий сетевого трафика. *Генная библиотека* такой искусственной иммунной системы должна содержать «гены» (это могут быть, например, данные о характерном количестве пакетов, их длине, структуре, типичных ошибках и т.д.), на основании которых будут генерироваться особые программные агенты – детекторы, служащие аналогами лимфоцитов. Начальные данные для формирования генной библиотеки выбираются, исходя из особенностей применяемых сетевых протоколов, в частности их слабых с точки зрения защиты мест. При обнаружении детекторами аномальной активности в сети к библиотеке в дальнейшем должны добавляться соответствующие этим проявлениям новые «гены». Следует заметить, что поскольку размер такой библиотеки ограничен, в ней должны сохраняться только «гены», проявляющиеся наиболее часто.

На втором этапе путем произвольного комбинирования «генов» происходит генерирование так называемых *пре-детекторов* (аналоги «зародышевых» лимфоцитов), которые затем с помощью механизма той самой негативной селекции проверяются на совместимость (или точнее, на несовместимость) с нормальным сетевым трафиком. При этом используются данные о характере такого трафика (профили), формируемые так называемым автоматическим профайлером (automated profiler), постоянно анализирующим поток данных, поступающий от маршрутизатора, стоящего на входе в сетевой сегмент.

Конечной целью в этом случае является создание ограниченного набора детекторов, с помощью которого можно было бы обнаружить максимальное число сетевых аномалий. Этот набор рассылается по узлам сети, образуя вторичную IDS.

Разработанные на сегодняшний день алгоритмы негативной селекции оперируют вероятностными характеристиками – вместо точного соответствия используется частичное, степень которого может произвольно варьироваться. Ее изменение в конечном итоге должно приводить к изменению (уменьшению или увеличению) частоты «ложных срабатываний».

При обнаружении аномалии происходит *клональная селекция* – соответствующий ей детектор «размножается» и рассылается на все узлы. Окончательное же решение о том, происходит вторжение в сеть или нет, принимается на основании данных от нескольких узлов. Каждый узел, а также основная IDS снабжены еще одним компонентом – «коммуникатором», который, в частности, оперирует таким параметром, как уровень риска. В случае, если на каком-то узле замечена подозрительная активность, коммуникатор поднимает свой уровень риска и отсылает соответствующее сообщение коммуникаторам других узлов и основной IDS, и те также поднимают свои уровни риска. При появлении аномалий сразу на нескольких узлах в течение короткого промежутка времени этот уровень очень быстро растет, и если будет достигнут заданный порог, администратор сети получит сигнал тревоги.

Можно отметить очевидное сходство между AIS и искусственными нейронными сетями: например, и те и другие способны изучать динамику и статистические свойства наблюдаемой системы, для достижения максимальной эффективности и в том и в другом случае необходимо подбирать значения управляющих параметров и т.д. В то же время имеется и ряд существенных отличий, являющихся в первую очередь следствием различия между имитируемыми системами – нервной и иммунной. Здесь первая состоит из фиксированных элементов (нейронов), а вторая – из блуждающих (лимфоцитов), первая управляется одним центральным органом (мозгом), а второй подобное «централизованное» управление не свойственно, в первой взаимодействие между элементами является постоянным, а во второй носит кратковременный характер и т.п.

Следует отметить, что в мире масштабные исследования в области искусственных иммунных сетей ведутся относительно недавно – большинство работ по данной тематике относится к 90-м годам. Так, ученые Лондонского Королевского колледжа сообщили о разработке в рамках проекта The Computational Immunology for Fraud Detection (CIFD) защитной системы для Internet на базе AIS. Предполагается, что на завершение указанного проекта уйдет еще около трех лет. Первым пользователем системы обнаружения вторжений, реализующей функции AIS, должна стать почтовая служба Великобритании.

В Рссии над созданием ОС с кибериммунитетом много лет работали специалисты известной компании «Лаборатория Касперского».

В 2017 году компания выпустила (https://informburo.kz/stati/chto-takoe-kiberimmunitet-i-kak-eto-rabotaet-rasskazyvaet-evgeniy-kasperskiy-.html) собственную безопасную операционную систему, которой не нужен антивирус. В ее основе заложена микроядерная архитектура. Система состоит из микрокомпонентов, и каждое взаимодействие между ними проходит через свой уровень безопасности. При этом функции каждого компонента строго ограничены узким набором действий.

«Если это турбина, у нее нет доступа в Интернет. Каждый модуль системы работает по строго определенным правилам. Взломать эту систему можно только

одним способом: заразить исполнителя, проникнув в компанию разработчика. То есть взломать исходный текст. При этом для хакеров велик риск, что их поймают в процессе взлома», – отмечает Евгений Касперский.

На момент выхода книги новой защитной системой в России пользуется компания по производству роутеров и сетевого оборудования Kraftway. Также она применяется в проекте одного из «умных» районов в Москве по сбору больших данных.

Основываясь на материалах блога «Лаборатории Касперского» рассмотрим более подробно принципы построения и основные инструменты этой ОС, позиционируемой разработчиками как «ОС с кибериммунитетом».

4.3.3. KasperskyOS – первая российская операционная система с кибериммунитетом

В мае 2020 г. известная практически всем специалистам по кибербезопасности российская компания «Лаборатория Касперского» анонсировала завершение своего нового амбициозного проекта – разработку полностью «безопасной» операционной системы ***KasperskyOS***. Конечная цель этого проекта – создать такую ОС, у которой был бы «кибериммунитет», поэтому ей не страшно будет доверить управление «умными» автомобилями, сложными техническими процессами и важными информационными системами (https://habr.com/ru/article/499746/).

Как известно, сегодня в мире существуют различные операционные системы (ОС) практически под любые задачи. Есть ОС общего назначения, такие как Windows, macOS или дистрибутивы на базе ядра Linux. Есть специализированные – для авиации и промышленности, с real-time-характеристиками и доказанной (подтвержденной опытом эксплуатации) надежностью. Но, к сожалению, полностью безопасных с точки зрения устойчивости к кибервоздействиям, т.е. имеющих «кибериммунитет», среди них пока нет. Справедливости ради надо сказать, что ряд экспертов высказывают сомнения о возможности создания сегодня подобной ОС.

Как мы показали в предыдущих главах, обычно различные меры защиты разрабатываются в ответ на существующие или потенциальные (известные) угрозы. Но этот подход тоже не дает 100% гарантий, поскольку, как мы видим, постоянно возникают все новые классы и виды угроз, которые разработчики ранее не знали.

Классический пример – широко распространенная техника возвратно-ориентированного программирования (return-oriented programming). Ведь еще совсем недавно абсолютное большинство экспертов полагали, что исполнение вредоносного кода станет невозможным, если только выполнить 2 условия:

- запретить исполнение кода в областях, куда могут попасть пользовательские данные;
- защитить от модификаций области памяти, где находится программный код.

Как теперь известно, это никак не помешало сотням хакеров найти способ «обойти» защиту с помощью подмены адреса возврата из процедуры и используя части кода самого приложения и системных библиотек.

Принимая во внимание свой богатый опыт работы в области расследования и предупреждения киберпреступлений в «Лаборатории Касперского» решили подойти к проблеме радикально: разработать свой оригинальный подход, обеспечивающий надежную защиту от любых атак – как известных, так и перспективных.

В основу этого проекта были положены следующие ***ключевые идеи*** (https://habr.com/ru/article/499746/).

Во-первых, а как можно понять, безопасно выбранное решение или нет? Нужно с самого начала установить конкретные цели безопасности – требования, выполнение которых должно обеспечиваться ***при любых сценариях работы системы***. Следовательно, в таком «безопасном» решении нужно сделать невозможным выполнение любых операций, способных повлиять на достижение целей безопасности.

Поэтому в процессе работы каждого решения нужно проверять, способна ли та или иная операция каким-либо негативным образом повлиять на безопасное функционирование системы, и если да, то такую операцию необходимо надежно блокировать. Однако здесь есть две непростые проблемы: ведь нам нужно понять, какие именно операции надо контролировать, и, соответственно, разработать методики оценки влияния этих операций на «безопасную» работу системы.

Известно, что начиная еще с 70-х годов прошлого века различными коллективами специалистов по информационной безопасности проводилась активная разработка все новых и новых принципов создания безопасных систем, и сегодня разрабатываются различные формальные математические модели разделения решений на домены с различным уровнем доступа.

В одной из предыдущих глав мы упоминали о подходе Multiple Independent Levels of Security (MILS). Он предусматривает разделение системы на отдельные изолированные домены безопасности и контроль всех операций, связанных с передачей данных между этими доменами. Именно на этом подходе базируется большинство современных «высоконадежных» систем.

Как мы уже говорили, если использовать набор таких полностью изолированных программных компонентов, то каждый из них в отдельности безопасен только до тех пор, пока они не взаимодействуют друг с другом и окружающим миром. Ни «кривой» код, ни уязвимости в этих отдельных компонентах не страшны операционной системе. Однако на практике для выполнения функциональных задач различные компоненты ПО неизбежно должны взаимодействовать как между собой, так и с внешним миром. Для того чтобы поведение системы по-прежнему оставалось безопасным, все подобные взаимодействия компонентов должны проводиться под жестким контролем с использованием следующих трех основных правил (https://habr.com/ru/article/499746/).

1. Сформулировать четкие гарантии обеспечения надежной изоляции компонентов друг от друга в системе. В MILS-системах, как известно, за эту задачу отвечает специальный инструмент – ядро разделения (Separation Kernel). На практике эту функцию выполняет микроядро или гипервизор.
2. Конкретно описать, как каждый отдельный программный компонент может взаимодействовать с другими. Тогда в результате появится возможность перечислить все подлежащие контролю операции.
3. Сформировать в системе специальный дополнительный компонент-медиатор, только через который будут проходить абсолютно все взаимодействия. Тогда у него будет возможность *разрешать безопасные* операции и *запрещать опасные*. Решение о том, какая именно операция является безопасной, принимается еще одним отдельным компонентом – вычислителем вердиктов безопасности (Policy Decision Point).

Справедливости ради надо отметить, что это не собственная идея «Лаборатории Касперского» – впервые отделить логику вычисления вердиктов (Policy Decision Point) от их применения (Policy Enforcement Point), как нам известно, было предложено еще в 90-е годы в рамках проекта Flux Advanced Security Kernel (FLASK).

Поскольку, по определению, Policy Decision Point автоматически принимает решения, от которых зависит безопасность всей системы, правила вычисления вердиктов должны быть однозначны и математически корректны. Для этого в команде «Лаборатория Касперского» создали специальный компилятор, который принимает на вход декларативные описания взаимодействующих компонентов и конфигурацию безопасности.

Итоговый результат работы такого компилятора – специальный программный код на языке C, определяющий функциональность Policy Decision Point. У этого автоматически генерируемого кода есть несколько преимуществ (https://habr.com/ru/article/499746/).

1. Доверие к такому коду выше, чем к написанному вручную. Например, вместе с кодом, сгенерированным на основе формальной модели, одновременно можно сгенерировать и набор тестов, проверяющих его соответствие модели. Упрощается и процесс формального доказательства определенных свойств полученного кода, например предельного времени выполнения.
2. Становится возможным использовать достаточно простые наборы правил взаимодействия компонентов между собой. Корректная работа правильно спроектированной системы предполагает использовать лишь малое число стандартных потоков исполнения, которые требуется описывать. В то же время конкретные правила вычисления вердиктов могут быть достаточно сложными и разнообразными – это уже забота компилятора.
3. Инженер по кибербезопасности описывает поведение системы в тех же терминах, с применением которых она была спроектирована, поэтому всегда есть возможность всесторонне учесть специфику каждого конкретного решения.
4. Описание безопасности выполняется независимо от бизнес-логики решения.

В итоге и появился такой «движок», который выполняет вычисление вердиктов безопасности, – Kaspersky Security System (KSS).

Разработчики KasperskyOS поясняют, почему они не взяли, например, Linux или другую операционную систему следующим образом (https://habr.com/ru/article/499746/).

Прежде всего – на базе существующей ОС Linux уже создано несколько механизмов и модулей безопасности: SELinux, AppArmor, GR security, SMACK, контейнеры и т.д. Однако все они оказываются абсолютно бесполезными, когда скомпрометировано ядро ОС. Linux – классическое монолитное ядро, где все компоненты работают в одном адресном пространстве и могут влиять друг на друга. Хотя код ядра Linux «просматривают миллионы глаз», но по-настоящему тщательной ревизии подвергаются только наиболее ответственные компоненты ядра. В ядре Linux более 15 млн строк кода, и понятно, что значительная его часть так и остается вне зоны пристального контроля Linux-сообщества. В результате, как известно, часто обнаруживаются критичные уязвимости, эксплуатация которых позволяет так или иначе скомпрометировать ядро Linux. Тем самым не реализуется главное

требование по обеспечению безопасности – изоляция между доменами. Цитата из https://habr.com/ru/article/499746/: «Кардинально поменять архитектуру Linux вряд ли получится, уж если у Таненбаума не получилось переубедить Торвальдса, то у нас и вовсе шансов нет».

В существующих микроядерных операционных системах ядро обычно весьма компактно и благодаря этому лишено описанных выше недостатков, свойственных «монолитным» и «гибридным» архитектурам. Микроядра идеально подходят для создания ядер разделения в MILS-системах. Более того, уже есть несколько хороших защищенных микроядерных операционных систем с открытым исходным кодом, например seL4.

Несмотря на все очевидные плюсы использования готового микроядра, специалисты лаборатории пришли к выводу, что все-таки возможности существующих систем в области безопасности недостаточны. Обычно создатели ОС пытаются контролировать доступ к ресурсам. Именно ресурсами в первую очередь оперирует модель безопасности object-capability, которая используется в большинстве микроядерных операционных систем. Дальнейшие «более изощренные» свойства безопасности обычно реализуются в виде прикладной логики. Возможности политик безопасности были бы сильно ограничены, если бы за основу взяли только модель object capabilities.

Таким образом, эксперты лаборатории пришли к принципиальному выводу, что использование «готовых» ОС не позволяет реализовать задуманную ими идеальную среду для работы KSS, и им пришлось в итоге разрабатывать новую операционную систему.

В основе KasperskyOS лежат следующие принципы (https://habr.com/ru/article/499746/).

1. ***Микроядерная архитектура.*** Чем компактнее ядро ОС, тем проще его исследовать и тем меньше возможностей для возникновения различных уязвимостей.
2. ***Минимально возможная поверхность атаки на ядро ОС.*** Так называемая поверхность атаки на ядро ОС определяется количеством системных вызовов и других возможных каналов внешних деструктивных воздействий. Но если архитектура «микроядерная», то в ядре нет драйверов, оно не взаимодействует через оборудование с внешними источниками воздействий. В этом случае поверхность атаки зависит лишь от количества используемых системных вызовов. У KasperskyOS всего 3 вызова не контролируются монитором безопасности – это вызовы, конкретно отвечающие за IPC. Для сравнения, у другой известной распространенной микроядерной ОС – QNX – их 116.
3. ***Гарантии изоляции.*** Необходимо исключить любую возможность обмена данными между процессами в обход KSS. Это зона ответственности микроядра операционной системы.

Все эти составляющие в сумме и позволили создать ОС с высоким уровнем безопасности.

Конечно, разработчики указывают на тот факт, что не всякое решение, созданное с применением KasperskyOS, безопасно по определению. Его необходимо правильно спроектировать. Для начала нужно определить именно те свойства решения, наличие которых мы считаем критичным с точки зрения безопасности.

Исходя из данных требований, функциональность решения нужно разбить на изолированные компоненты, определить все возможные варианты их взаимодействия и, наконец, описать политики безопасности так, чтобы поведение системы оставалось действительно безопасным в любых ситуациях.

Часть компонентов при этом могут быть «недоверенными», на гарантии безопасности решения в целом это не повлияет. Отдельные компоненты могут быть атакованы, но в такой правильно спроектированной системе атака не приведет к нарушению этих гарантий, даже если злоумышленник и получит возможность выполнять произвольный код. Именно это свойство информационной системы разработчики ОС и называют ***кибериммунитетом***.

Основные области применения KasperskyOS:

- логические контроллеры для:
  - транспортных систем;
  - АСУ ТП;
  - энергетических систем;
- интернет вещей;
- автомобили;
- сетевое оборудование;
- встраиваемая электроника;
- доверенные рабочие станции для работы с конфиденциальной информацией.

Так, например, Kaspersky Mobile Security SDK – это модуль для защиты сервисов и мобильных устройств, работающих на операционных системах Google Android, например, в Infotainment автомобиля или мобильном устройстве его пользователя.

SDK предоставляет широкий спектр функций для обеспечения безопасности, которые могут быть интегрированы в конкретное приложение пользователя:

- обнаружение вредоносного ПО;
- антифишинг & защита от Fake-приложений;
- защищенное соединение;
- репутация устройства;
- защита данных;
- самозащита;
- антивор.

Kaspersky Security for In-Vehicle Infotainment (IVI) выполняет контроль портов и коммуникаций, контроль приложений, обеспечивает интеграцию с внешними устройствами.

- Контроль портов устройств:
  - антивирусная защита для USB-накопителей (KSN) ;
  - защита от BadUSB-атак;
  - блокировка внешних диагностических сеансов (OBD-II).
- Контроль коммуникаций:
  - репутация Wi-Fi точек доступа (KSN), защита от атак их подмены;
  - система предотвращения вторжений (Virtual patching).
- Контроль приложений:
  - hardening приложений, контроль поведения (KSN) ;
  - обнаружение подозрительной деятельности на основе машинного обучения.

- Интеграция с внешними системами:
  – противоугонная защита автомобиля (геолокация, блокировка, очистка данных) ;
  – Fleet Management systems (местоположение, события) ;
  – интеграция с SOC: «охота» на угрозы и расследование инцидентов.

4.3.4. Киберфизические иммунные системы

Здесь очень кратко рассмотрим основные направления развития безопасных киберфизических систем (Cyber-Physical System – CPS). Проблема в том, что проектировщики информационных систем даже таких крупных CPS, как промышленные и электроэнергетические системы, изначально практически не уделяли особого внимания проблеме их *безопасности* – приоритет был отдан *функциональности* составных компонентов, их совместимости и обеспечению способности надежно функционировать в течение длительного периода времени с учетом перегрузок и дестабилизирующих факторов.

Но с изменением ландшафта угроз проблемы противодействия спектру атак, направленных на нарушение основных функций киберфизической системы (отключение электричества в мегаполисе, остановка производственной линии), выходят на первый план. В последнее время хакерские группы и даже субъекты национальных государственных структур стремятся сделать такие критические атаки на инфраструктурные объекты *ключевым компонентом своих стратегий кибервойны*.

Разнообразность и все возрастающая сложность этих атак выдвигают на высший приоритет проблему защиты CPS.

Как показано выше, сегодня нет недостатка в технологиях и подходах защиты данных, но эти подходы не работают против атак, которые происходят в физическом мире, включая атаки с использованием датчиков, исполнительных механизмов, преобразователей и контроллеров в физической среде. Меры безопасности по периметру, такие как брандмауэры и системы контроля доступа, могут сдерживать или предотвращать кибератаки, происходящие извне системы, но никак не защищают от внутренних атак, которые обычно инициируются агентами, хорошо знакомыми с атакуемой системой.

Большая работа была проделана при разработке систем обнаружения сетевых вторжений, но эти системы, как правило, обучаются медленно и, как правило, беспомощны против неизвестных и адаптивных угроз. Исследователи и практики сегодня согласны с тем, что для достижения высокой степени безопасности CPS необходимо будет комбинировать различные подходы, но пока неясно, как именно это будет достигнуто. Вот здесь эксперты и предлагают аналогию с иммунной системой человека.

Человеческое тело рассматривается как полностью саморегулируемая система. Когда человек ощущает некое «ненормальное» событие, такое как травма или инфекция патогенным микроорганизмом, он автоматически начинает задействовать различные защитные механизмы.

В течение эволюционного периода человеческое тело адаптировалось к обнаружению широкого диапазона аномалий – микроскопических патогенов, различных видов травм, аллергий и изменений в окружающей среде.

Например, можно считать, что *вакцины* являются эквивалентом обученных *систем обнаружения* вторжений. *Одежда* является эквивалентом охраны *периметра*. Тем не менее подавляющее большинство человеческих реакций являются непроизвольными и автоматическими, как будто тело поддерживает «модель себя» и знает, когда и как эта модель отклонилась от своего нормального состояния.

Одним из направлений современных исследований является переосмысление CPS с этой точки зрения иммунной системы. Чтобы создать *киберфизическую иммунную систему*, она, как и человеческое тело, должна стать «самоосознающей».

Чтобы построить достоверную модель своего собственного поведения, система должна не только изучать свое *цифровое* поведение, но и фиксировать поведение своих *физических подсистем*. Одним из способов достижения этого является представление поведения в терминах физических законов. Например, движущиеся части системы будут подчиняться законам механики; части подсистемы регулирования температуры будут подчиняться законам термодинамики; и электрические установки будут подчиняться законам электротехники и т.д.

Теоретически возможно определить соответствующие физические величины, применить соответствующие физические законы и затем обнаруживать отклонения от ожидаемого поведения. Эти отклонения предполагают, что система может функционировать ненормально из-за собственного износа, спонтанного отказа или целенаправленной злонамеренной деятельности. Обнаружение «аномалий», в принципе, работает таким образом.

Однако здесь возникает одна большая проблема – описанный выше подход должен обязательно выходить за пределы узкого «сообщества безопасности».

Традиционно кибербезопасность была делом только инженеров по безопасности, сетевых администраторов и криптографов. Но для создания подобной киберфизической иммунной системы необходимо тесно взаимодействовать с другими многочисленными экспертами, которые работают над ее, образно говоря, «не кибераспектами».

К ним относятся прежде всего ученые – прикладные физики, инженеры-химики, теоретики систем адаптивного управления, биологи и другие эксперты в своей узкой «дисциплинарной» области, которые могут создавать и связывать между собой модели различных физических и компьютерных подсистем, а также квалифицированно рассуждать об отклонениях от «безопасного» поведения.

Чтобы реализовать пока еще мечту о киберфизической иммунной системе, на практике требуется не что иное, как *действительно междисциплинарное сотрудничество* (http://unetway.com/news/sozdanie-kiberfiziceskoj-immunnoj-sistemy/).

Напомним, что киберфизические системы (Cyber-Physical System, CPS) – это системы, состоящие из различных физических объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое. В CPS обеспечивается тесная связь и координация между *вычислительными* и *физическими* ресурсами. Компьютеры осуществляют мониторинг и управление физическими процессами с использованием такой петли обратной связи, где происходящее в физических системах оказывает влияние на вычисления, и наоборот.

Чрезвычайная сложность такого рода задач говорит о том, что здесь речь не идет о создании автоматизированных систем, более крупных, чем существующие, где

компьютеры интегрированы или встроены в те или иные физические устройства или системы. Речь идет о гармоничном и синхронном сосуществовании двух типов моделей. С одной стороны – это традиционные «инженерные» модели (механические, строительные, электрические, биологические, химические, экономические и другие), а с другой – модели «компьютерные».

В этом смысле предшественниками CPS можно считать встроенные системы реального времени, распределенные вычислительные системы, автоматизированные системы управления техническими процессами и объектами, беспроводные сенсорные сети.

С технической точки зрения CPS имеют много общего со структурами типа грид, реализуемыми посредством Интернета вещей (Internet of Things, IoT), Индустрии 4.0, промышленного Интернета вещей (Industrial Internet), межмашинного взаимодействия (Machine-to-Machine, M2M), туманного и облачного компьютинга (fog и cloud computing). Но этими техническими средствами ни в коем случае нельзя ограничивать представление CPS. Для этих сложных систем требуются новые кибернетические подходы к моделированию, поскольку именно модели являются центральным моментом в науке и инженерии.

Здесь имеет смысл привести результаты исследований Академии Acatech.

Организованная в 2008 г. немецкая академия наук и новых разработок Acatech-Deutsche Akademie der Technikwissen-Schaffen позиционирует себя как нейтральное учреждение, формирующее советы (прогнозы) политикам, ученым и производственникам по ключевым проблемам науки и техники, публикуя свои советы (прогнозы) в виде отчетов по результатам исследований.

В последних отчетах Acatech уже уверенно говорится о реальных перспективах появления *национальных киберфизических платформ*, которые будут складываться из трех типов сетей:

- Интернет людей.
- Интернет вещей.
- Интернет сервисов.

По мнению немецких академиков, перспективы появления киберфизических систем и формирования на их основе Индустрии 4.0 затрагивают интересы общества в целом, поэтому должны рассматриваться не только в техническом, а в более широком социокультурном аспекте, с учетом демографических и других происходящих изменений.

В качестве аргумента против мнения ряда критически настроенных экспертов о том, что это просто «лозунги немецких академиков», можно привести такие факты. В США это направление (киберфизические платформы и системы) с 2011 г. официально включено в состав важнейших и перспективных «стратегических» технологий.

В государстве Сингапур на законодательном уровне принята к исполнению инициатива (комплексный проект) «Умная нация», которая подразумевает социальное и экономическое развитие государства с ориентацией на базовые киберфизические платформы.

Очень активно работает в этом направлении Китай и многие европейские страны.

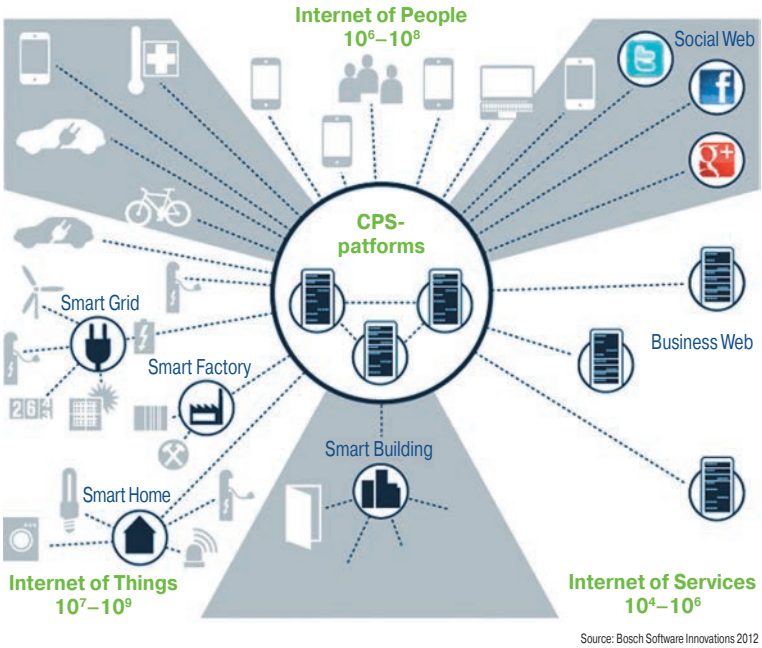

Рис. 4.2. Киберфизические системы возникают на стыке Интернета людей, вещей и сервисов

Что касается России, то пока особой активности в этом направлении не наблюдается, за исключением некоторого роста числа публикаций (в основном обзорного характера) по отдельным теоретическим аспектам создания киберфизических систем.

Область применения CPS распространяется практически на все виды человеческой деятельности, включая все многообразие промышленных систем, транспортные, энергетические и военные системы, все виды систем жизнеобеспечения от медицины до умных домов и городов, а также многие экономические системы.

Мы полагаем, что создание полноценных иммунных (кибербезопасных) систем CPS в перспективе приведет примерно к таким же изменениям во взаимодействии с физическим миром, как те, к которым привела в свое время Всемирная сеть (https://www.tadviser.ru/index.php/).

4.3.5. Биометрическая система кибербезопасности Darktrace

Один из мировых лидеров в этой сфере – созданная в 2013 г. английская компания Darktrace, среди учредителей которой большинство бывших британских разведчиков, которые прекрасно осведомлены о реальных масштабах и перспективах киберугроз.

Основной продукт компании – подключаемый к сети специальный сервер, распознающий и автоматически реагирующий на любые скрытые угрозы – благодаря машинному обучению система замечает вещи, которые сегодня игнорируются стандартными антивирусами и фаерволами.

Так, британская компания Darktrace, работающая в сфере кибербезопасности, концепции построения своих программных продуктов во многом заимствует у биологических объектов. Свой подход специалисты на сайте компании описывают следующим образом:

«На нас постоянно воздействуют миллиарды микробов и бактерий, однако у нас есть иммунитет, который позволяет нам эффективно справляться со всеми подобными рецидивами прежде, чем они успеют переродиться во что-то, что причинит нам ущерб. Эта постоянная работа иммунитета не побеждает все зло в организме, но держит ситуацию под контролем – ущерба для организма нет. Роль известного специалистам по ИБ термина «периметр защиты» у нас выполняет кожный покров, защищающий нас от этой агрессивной среды. Ведь точно так же, как специалисты по ИБ постоянно смотрят за периметром, мы соблюдаем санитарную гигиену. Но если наш иммунитет ослабевает – мы заболеваем (получаем «ущерб»).

В человеческом организме идет бесконечная битва с вирусами. В ходе эволюции мы выработали надежные внутренние и внешние механизмы борьбы с этими угрозами – иммунную систему. Человеческая кожа и вовсе похожа на цифровой фаервол, который постоянно изменяется, совершенствуется и укрепляется.

В сфере кибербезопасности разрушение одного барьера приводит ко всему краху системы. Не хватает такой «иммунной системы», которая постоянно отслеживала бы состояние устройства и автоматически реагировала бы на любое отклонение от нормы. Ведь вирусы и сторонние агенты постоянно видоизменяются – как в биологии, так и в IT-сфере».

Впервые о понятии «кибериммунитета» заговорили еще в 80-е годы. Но тогда искусственный интеллект находился в зачаточном состоянии и не мог помочь ученым создать подобную новую технологию. Сегодня же при помощи алгоритма ИИ и машинного обучения можно попытаться воспроизвести две основные черты биологической иммунной системы – память и способность обучаться. Именно на этом направлении и специализируется Darktrace.

Подобный алгоритм составляет основу модели каждого устройства, чтобы понять нормальный механизм его работы. Так программа вырабатывает интерфейс для визуализации угроз. Как и биологический иммунитет, Darktrace отсеивает лишние шумы, концентрируясь на главном. Система будто бы постоянно находится в спящем режиме и оценивает вероятность угроз, принимая во внимание любые переменчивые условия.

В случае же явной угрозы программа автоматически запускает механизм «горшочка с медом», т.е. как бы «захватывает» хакера и наблюдает за его поведением. Она изучает, откуда он, какую информацию ищет и что для этого делает.

Таким образом Darktrace выявляет подозрительную активность в сети, утечки паролей, перемещения файлов и вредоносные хакерские программы.

Конечно, у этого алгоритма есть и свои недостатки. Как человеческий иммунитет порой начинает «аутоиммунные атаки», так и приведенный алгоритм может принять за врага совершенно нормальные файлы. Более того, на этом могут сыграть высококвалифицированные хакеры. Они могут запрограммировать вредоносное ПО так, чтобы оно превращало базовые файлы в псевдоопасные. Тогда антивирусный алгоритм начнет с ними борьбу и, возможно, самих же их и уничтожит.

Так или иначе, кибербезопасность – это всегда игра в кошки-мышки, где нет понятия 100%-ной надежности. Однако, как считает большинство экспертов, биометрическая система кибербезопасности Darktrace находится на верном пути и использует правильные алгоритмы для своего развития.

На момент выхода книги компания предлагает потребителям обеспечить безопасность сети путем установки системы Enterprise Immune System – EIS. К корпоративной сети сегодня она может подключаться в двух вариантах: как аппаратное устройство и в виде виртуальной машины.

Завершая эту главу, можно сформулировать главный вывод – современные специалисты по кибербезопасности не только должны хорошо понимать специфику и правильно применять широкий спектр защитных инструментов (антивирусных программ и средств проактивной защиты), но при разработке или актуализации корпоративных концепций и стратегий кибербезопасности активно использовать и последние достижения в области иммунного подхода к защите ИТ-систем.

Литература к главе 4

1. https://www.comss.ru/page.php?id=1101
2. Алексеев А.П. Информатика. – М.: Солон-Р, 2002.
3. Острейковский В.А. Информатика. – М: Высшая школа, 2001.
4. http://www.ctc.msiu.ru/materials/Book1/contents.html
5. http://school.bakai.ru/inform/inform.htm