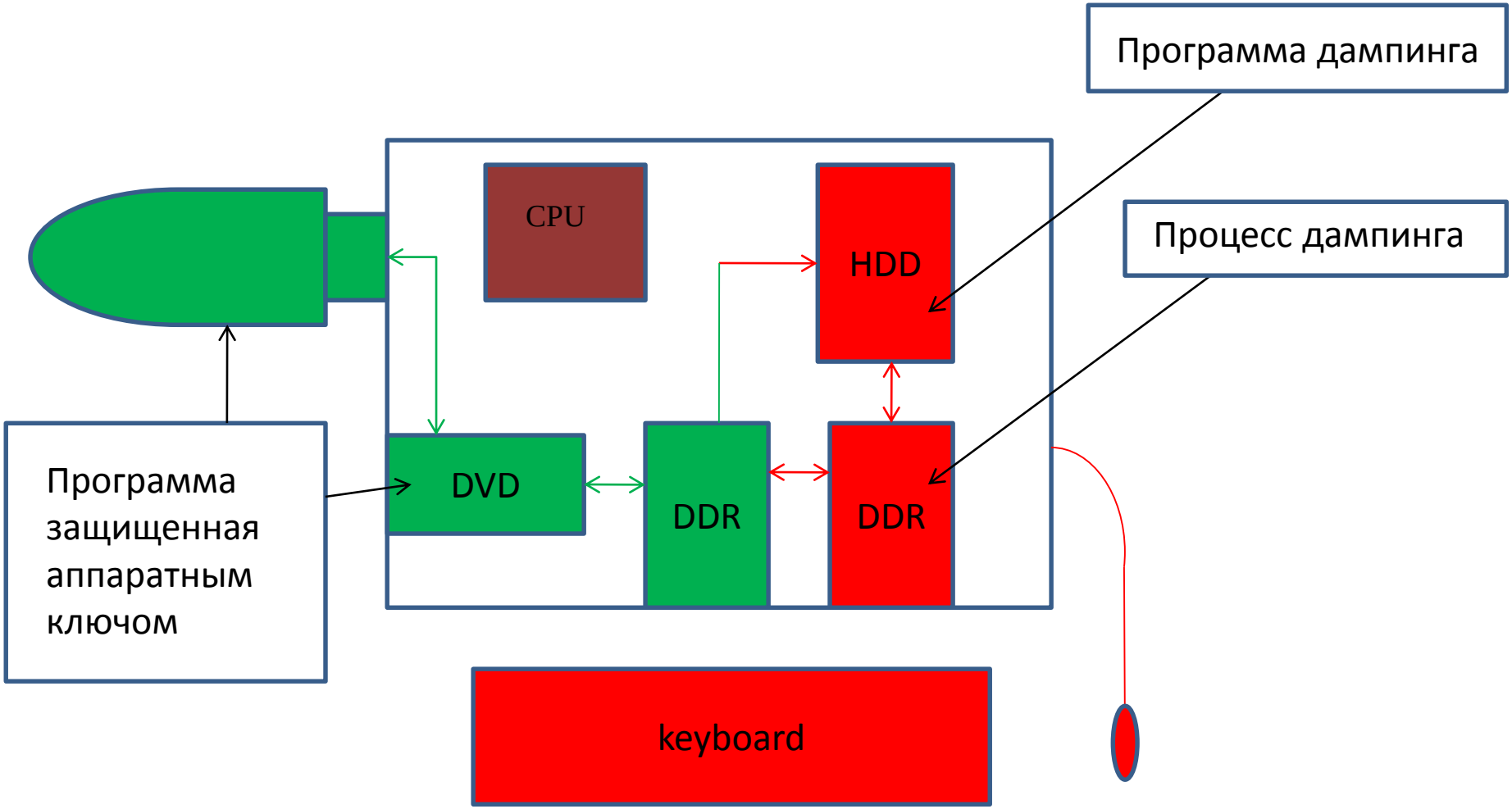
Как известно на сегодняшний день, компьютер предоставлен злоумышленнику в полной мере как он есть.

Все меры защиты, существующие на сегодняшний день, образуют локальную защищенную область в компьютере, которая стоит как крепость и соблазняет злоумышленника, предлагая ему применить весь арсенал компьютера и талантов злоумышленника.



Представляемая технология называется «Способ ограничения применения возможностей программных, аппаратных и программно-аппаратных ресурсов электронного устройства для защиты интеллектуальных прав».

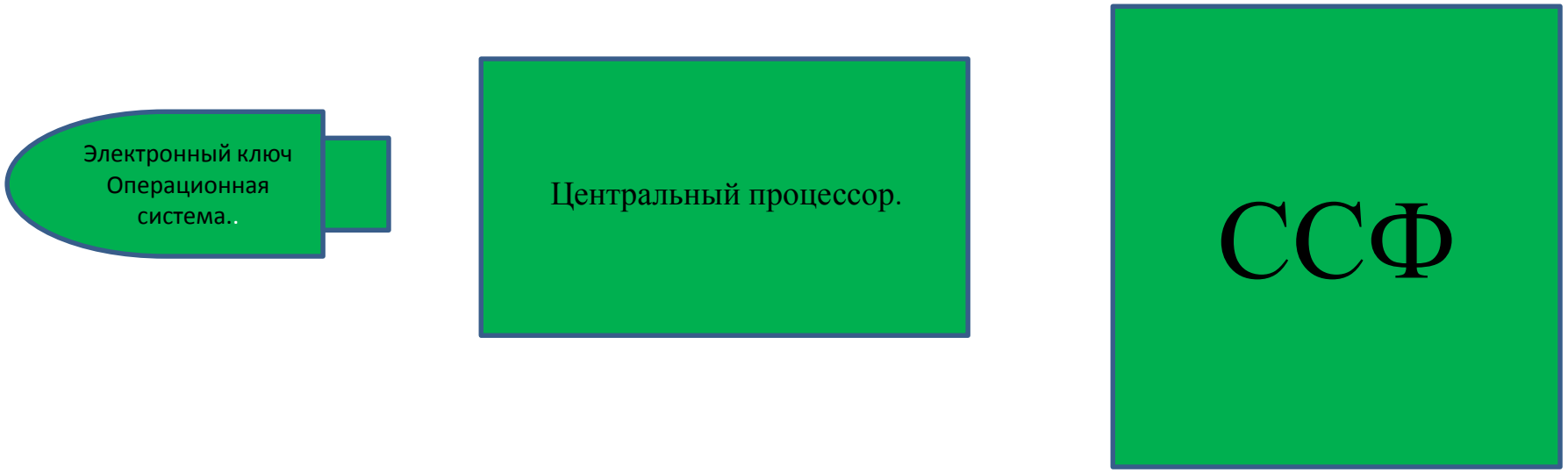
Смысл в том, чтобы перехватить контроль над устройством (компьютером) до того как контроль над устройством возьмет его владелец.

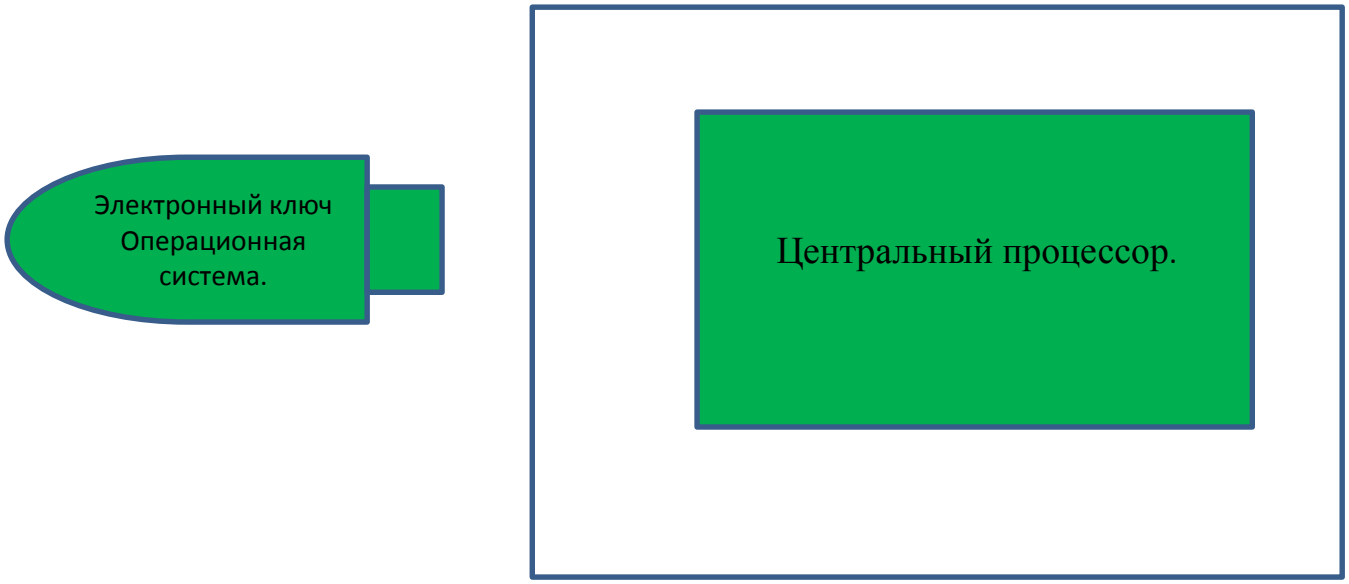
Основу составляют три ключевых компонента:

Электронный ключ, содержащий операционную систему.

Центральный процессор.

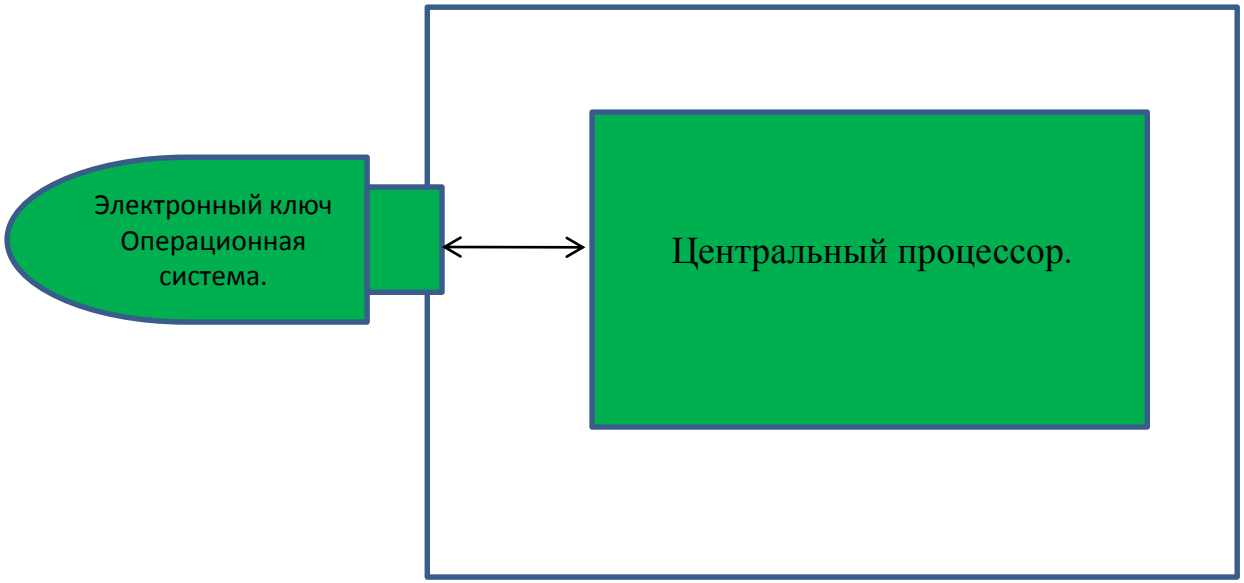
Сервер Содержащий Файлы (ССФ). (Защищаемые этим способом файлы)





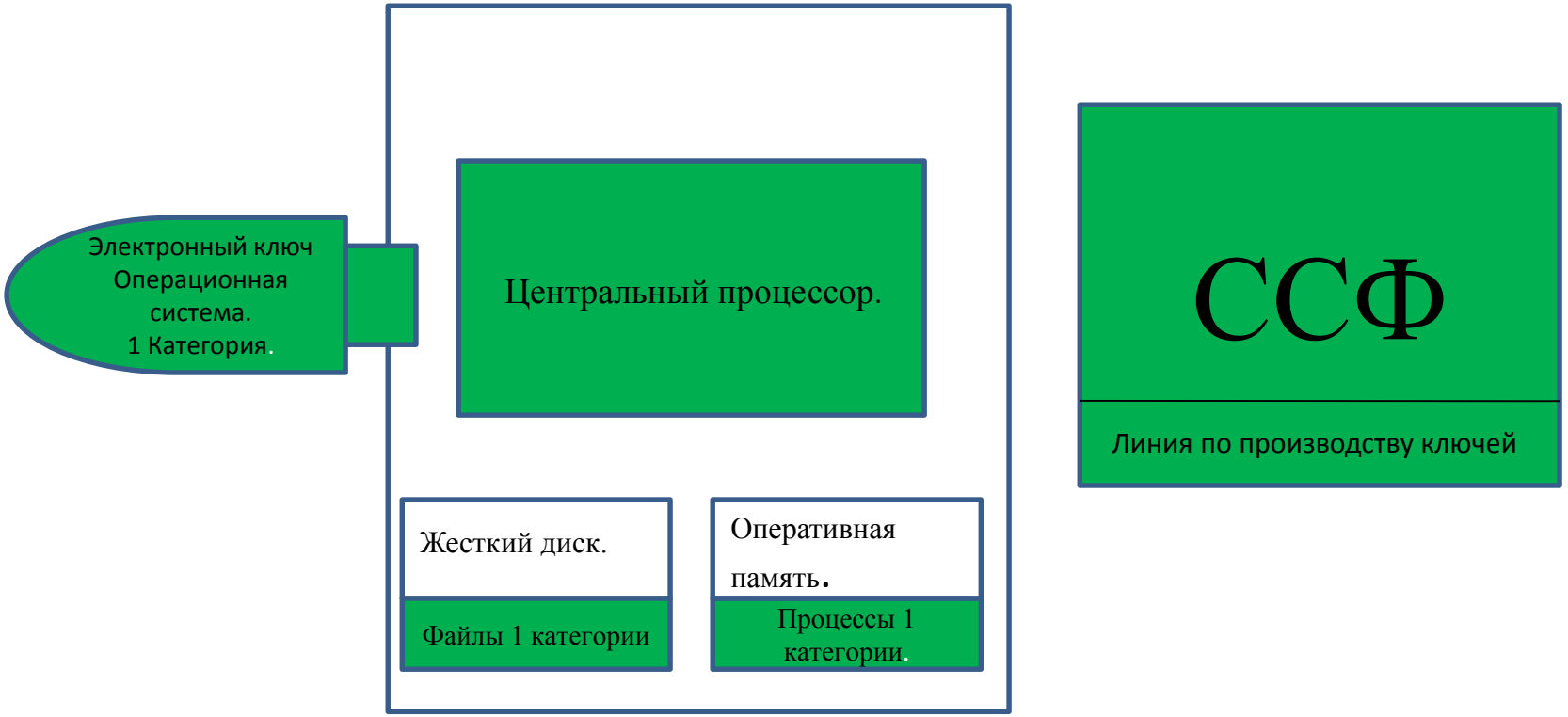
Предлагаемый способ организации защиты информации бьёт злоумышленника в самую основу. Он отсекает использование ресурсов компьютера в преступных целях. Компьютер просто невозможно включить без аппаратного электронного ключа. Т.е. не осуществляется даже процедура работы BIOS (POST), если к компьютеру не подключен аппаратный ключ.

По заявленному способу, при включении компьютера, центральный процессор первым делом проверяет USB-порты на наличие или отсутствие в них каких-либо устройств. Если никаких устройств не обнаружено, процессор отключает питание.



Если процессор обнаружил какое-либо USB-устройство, он отправляет ему зашифрованный вопрос, составленный с использованием случайных переменных по алгоритму, зашитому в процессор и известному ключу. Если ответ от ключа правильный, значит, обнаружен искомый ключ. Если ответа нет, значит, это устройство не ключ и питание отключается.

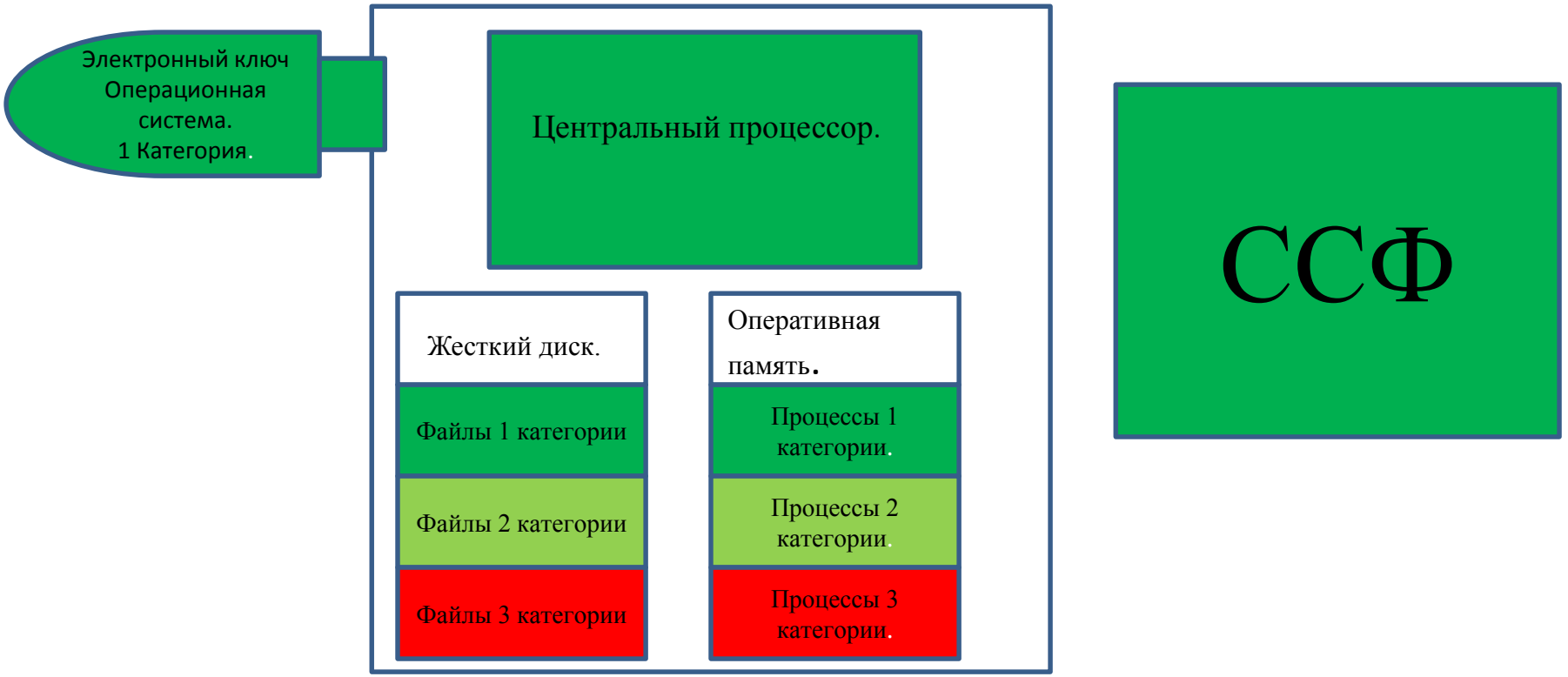
Если обнаруженное устройство ключ, то в дело вступает операционная система ключа. Она берет под контроль всё аппаратное обеспечение компьютера и каждый бит информации на нём, каждый электронно-вычислительный процесс. Контроль заключается в определении, что можно данному файлу и процессу, а что нельзя.



Файлы и процессы по заявленному способу делятся на три категории.

1 категория – это файлы, защищаемые заявленным способом и распространяемые из Сервера Содержащего Файлы в зашифрованном виде. Шифруются файлы для каждого ключа индивидуальным симметричным крипто-ключом. Процессы, основанные на файлах 1 категории, считаются процессами 1 категории. К 1 категории относится и операционная система ключа.

Для простоты изложения лучше будет представить, что линия по производству аппаратных ключей работает в одном здании, где расположен Сервер Содержащий Файлы. Это условие обеспечивает безопасную и безукоризненную работу симметричных ключей шифрования.



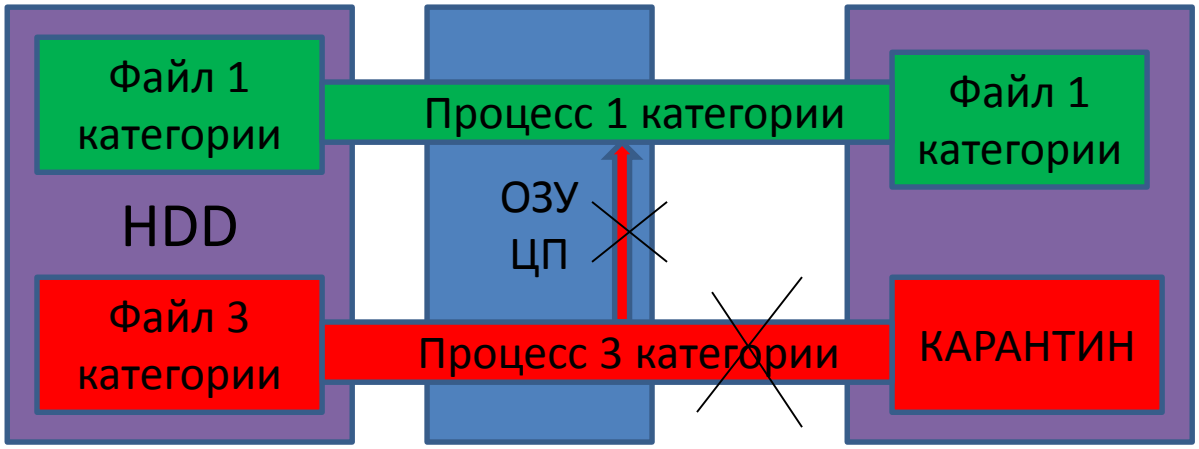
2 категория – это файлы, являющиеся производными файлов и процессов 1 категории. Процессы основанные на файлах 2 категории считаются процессами 2 категории.

Все остальные вообще, файлы и процессы, считаются файлами и процессами 3 категории. Не важно откуда они берутся, с клавиатуры, ДВД или из Интернета.

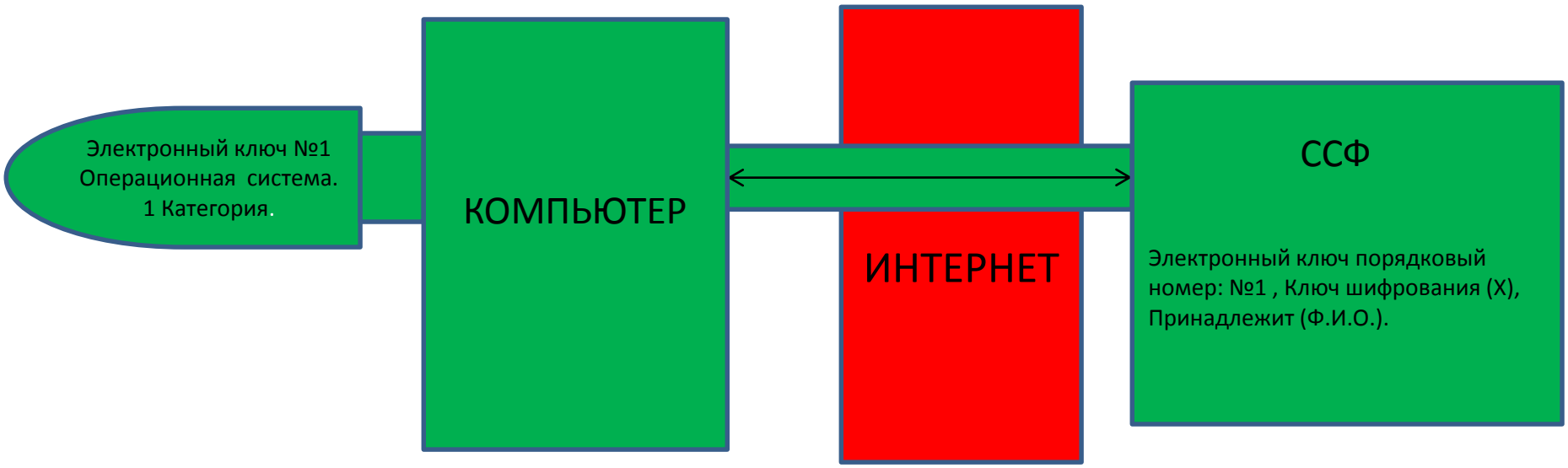
Операционная система ключа следит за тем, чтобы файлы и процессы 3 категории не воздействовали на файлы и процессы 1 и 2 категории.

Чтобы вторая категория на воздействовала на первую.

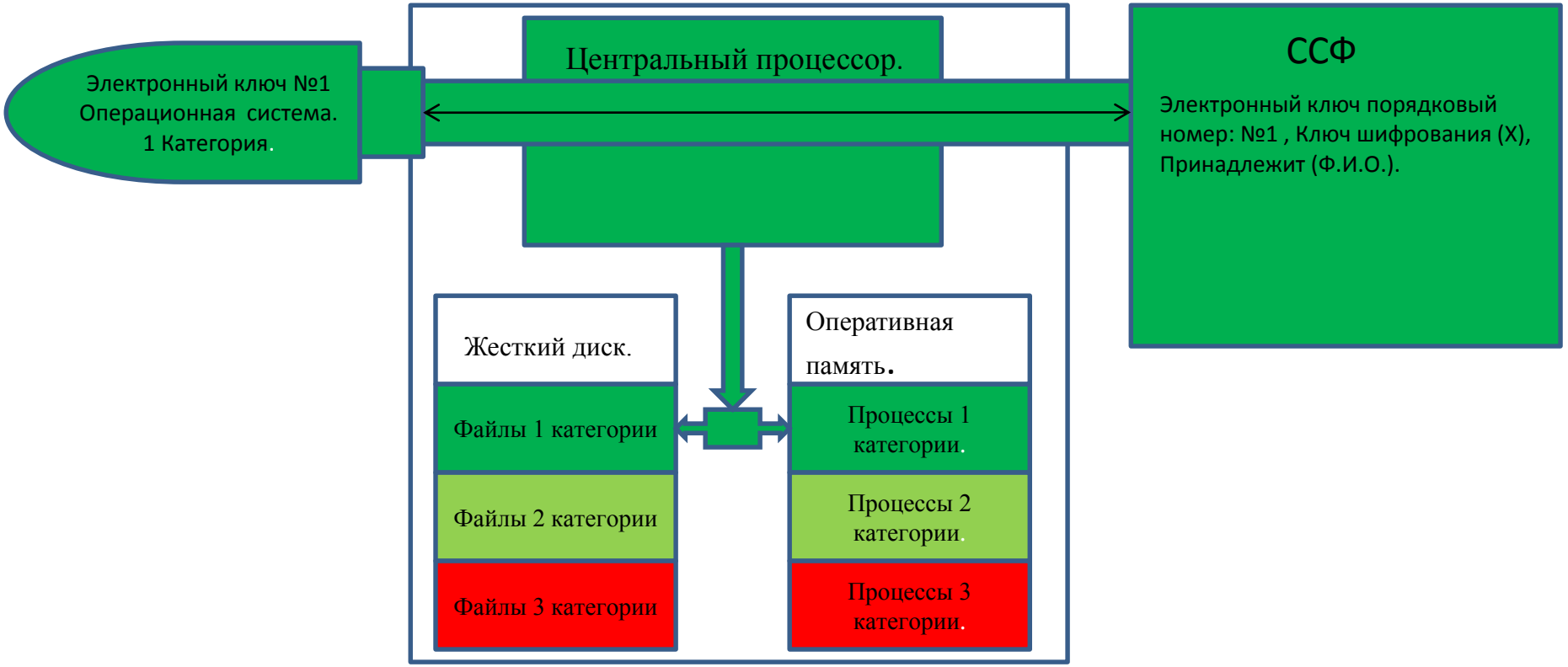
Под воздействием понимается взлом, копирование, отладка, декомпиляция, дизассемблирование, дампинг, удаление, внесение изменений и дополнений и т.п.



Операционная система не допускает взаимодействие процессов 3 категории с процессами 1и 2 категории путём прерывания процесса 3 категории. А при следующей попытке данного процесса 3 категории взаимодействовать с процессами 1 и 2 категории, данный процесс 3 категории прерывается, а файл 3 категории ранее инициировавший процесс заносится в карантин до последующего указания пользователем, что с ним делать. То же самое относится и к взаимодействию 2 категории с 1 категорией. При том, что 2 категория может воздействовать на 3 категорию.



Поскольку пакеты из ССФ в компьютер идут зашифрованными, постольку их перехват не даст перехватившему никакого толку. Ибо шифрование производилось многобитным симметричным ключом. Применение симметричного ключа целесообразно в данном способе защиты потому, что не надо куда либо перевозить или пересылать данные по ключу шифрования. Ведь производство аппаратных ключей осуществляется в одном здании где потом происходит шифровка на данный аппаратный ключ. А в сам аппаратный ключ залезть нельзя. В то же время известно, что сейчас развиваются методы взлома несимметричных ключей, путем подбора формул вычисляющих простые числа. Разумеется, при тех условиях применения симметричного ключа о которых идёт речь тут, симметричный ключ выглядит гораздо надежнее.



Сервер содержит все данные по ключам. Поэтому достаточно на чистом компьютере с помощью операционной системы ключа зайти на сервер и скачать на жесткий диск любой софт. Софт может быть расшифрован и установлен только с помощью ключа, на который происходила шифровка. Также как и работа установленного софта возможна только при контакте установленного софта с ключом производившим установку.

Это условие обеспечивает результат «Одна копия контента – один владелец».

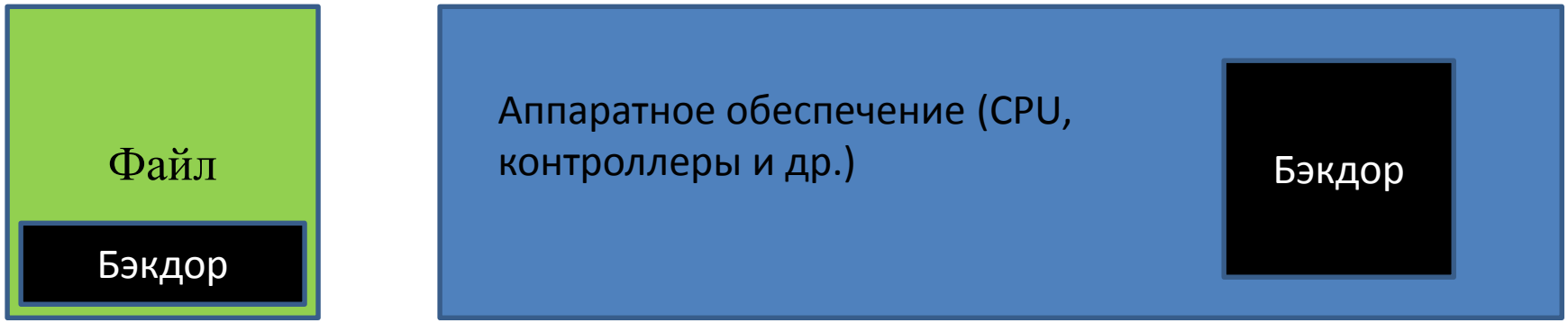
При этом, важно понимать, что операционная система ключа – это очень лёгкая программа, которая содержит код, необходимый для выполнения условий способа. Эта ОС может легко сосуществовать с другой, установленной на HDD полновесной операционной системой.

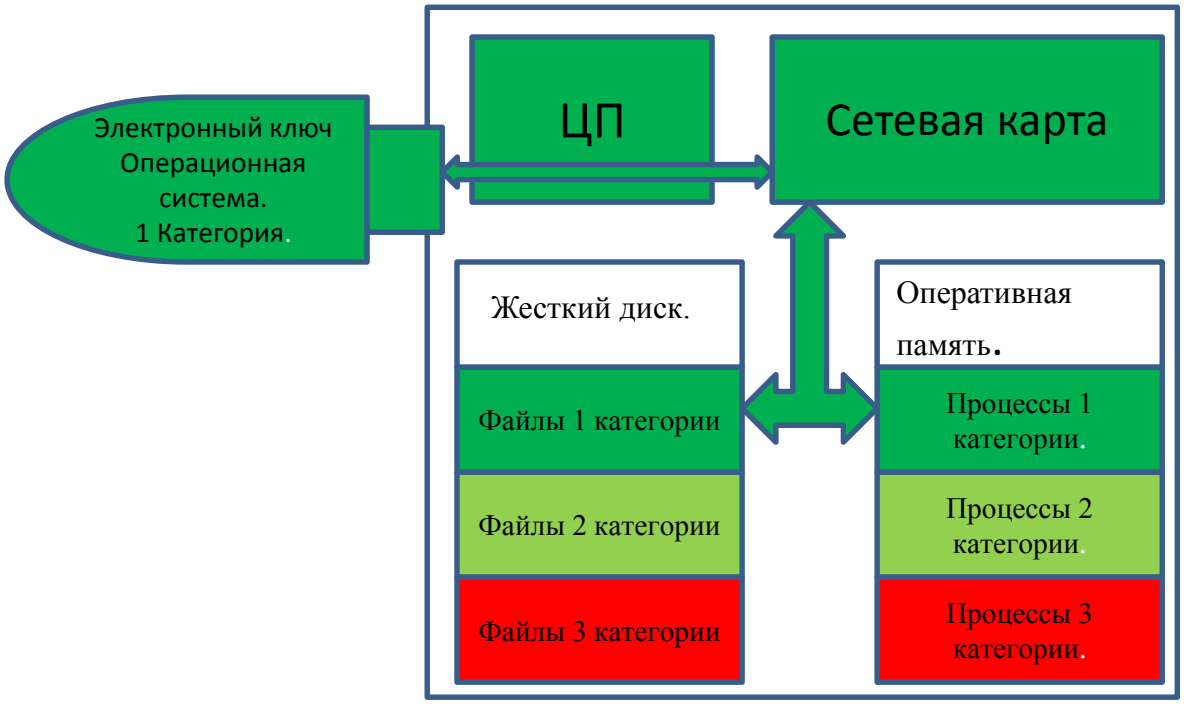
Конечно, существует множество опасностей в мире Информационных Технологий, множество видов атак и проникновений. К сожалению, в данный момент на каждый вид угрозы осуществляется практически индивидуальная мера защиты. Такая ситуация оставляет злоумышленнику возможность пользоваться ресурсами компьютера для взлома этих средств защиты.

Заявленный способ, эта технология, удачно представляет собой новую фундаментальную платформу, на основе которой легко разрабатываются новые непробиваемые приёмы защиты для любого вида угрозы. Ибо реализуется фундаментальный компонент – невозможность включить компьютер без контролирующего устройства, при том, что в контролирующее устройство проникнуть нет возможности.

ПРИМЕР:

Существуют так называемые «задние двери». Это закладки в виде программного кода, или в виде аппаратного свойства оборудования. С их помощью можно незаметно выводить информацию из компьютера в интернет. При этом антивирусное обеспечение может ничего и не заметить.

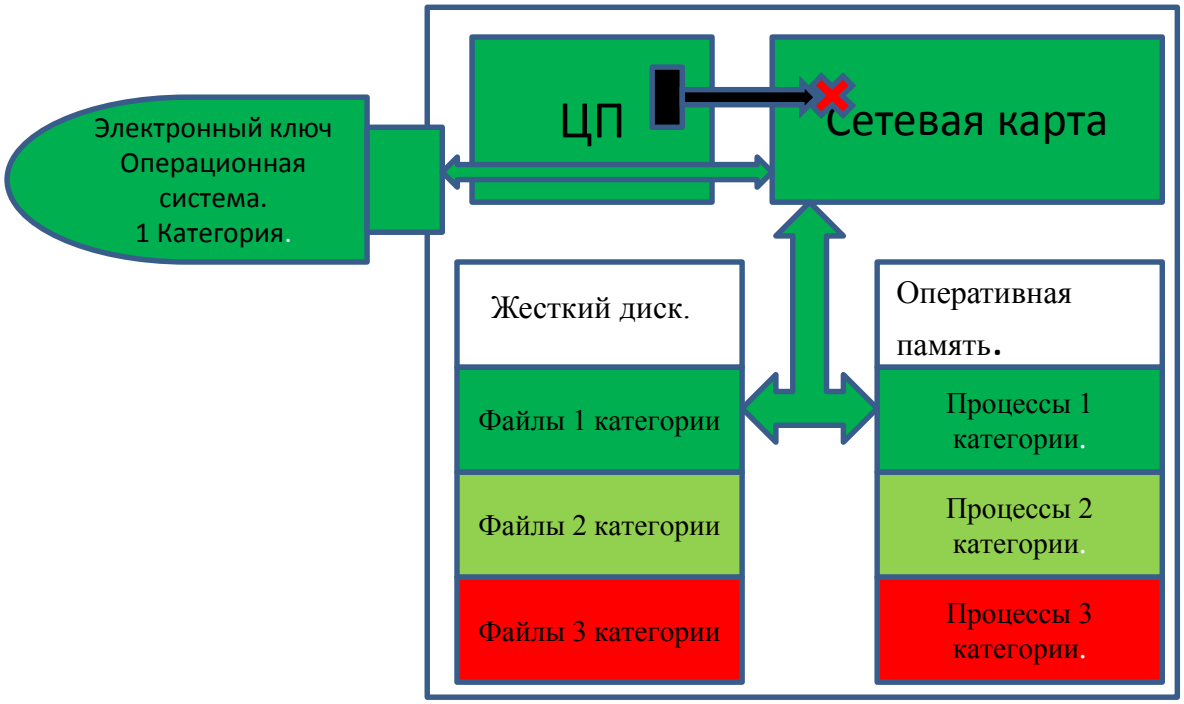




«Заслонка» представляет собой прием, который перекрывает возможность не санкционированного выхода информации из компьютера.

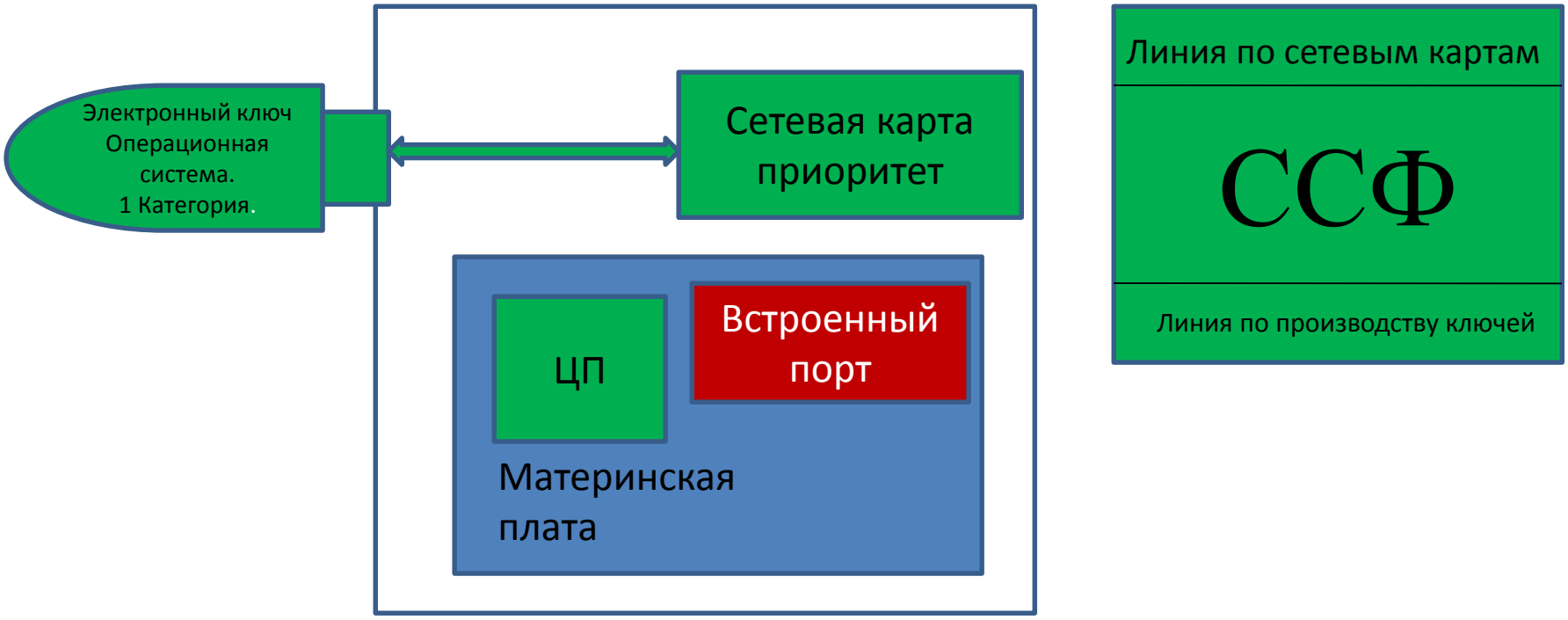
В здании, где располагается ССФ и линия по производству аппаратных ключей, устанавливается линия по производству сетевых карт. Эти карты предназначены не для создания локальной сети, а для выхода в сеть интернет.

Электронный ключ знает структуру карты (не зря они производятся в одном здании), и с самого начала работы компьютера, заносит в неё каталог известных ему процессов претендующих на выход в интернет и имеющих на это право. Право имеют только те приложения, которые предназначены для работы с сетью интернет. Все остальные право не имеют. Разумеется проще всего, когда право имеют только процессы 1 категории.



Представить наличие бэкдора в коде, при работе заявленного способа – трудновато. Даже если в ССФ такое ПО и пройдет, то при работе процесс будет зарегистрирован сразу как не предназначенный для работы с интернетом и заблокирован. Пользователь получит уведомление от системы ключа, а производитель ПО компрометируется.

Если же бэкдор аппаратная, и может за счет своих аппаратных ресурсов выходить в интернет минуя регистрацию в оперативной памяти, то поскольку процесс от аппаратного бэкдора операционная система ключа в каталог не вносила, постольку сетевая карта не выпускает его в интернет. И что проще, аннулирует этот процесс, заявляя пользователю о случившемся. Любой процесс из аппаратного бэкдора попадая в ОЗУ, опять таки оказывается в 3 категории. Это приводит к лёгкому выявлению аппаратного бэкдора.



Конечно, можно себе представить, что пользователь не захотел покупать сетевую карту производящуюся в ССФ, а захотел пользоваться выходом встроенным в материнскую плату. Но если законодательно для защиты госбезопасности ввести правило для провайдеров не взаимодействовать с клиентом у которого нет такой сетевой карты, то вопрос оказывается решенным. Либо обязать использовать такие сетевые карты только госучреждения, а пользователю оставить выбор. Но тогда надо реализовать в операционной системе ключа приоритетность такой сетевой карты перед стандартным выходом, если пользователь пожелает карту всё же установить.

Известно, что иногда коды операционных систем и приложений содержат уязвимости.

В мире, где царит этот фундаментальный способ защиты, даже при наличии таких уязвимостей, опасаться – смысла нет. Ибо средства для выявления таких уязвимостей и использования их, злоумышленнику будут не даны изначально.

Даже если злоумышленник приобретёт файл 1 категории программы-отладчика, или дизассемблера из сервера (ведь такие файлы тоже могут быть защищаемой интеллектуальной собственностью), то и в этом случае он не сможет использовать их возможности для своих зловредных целей. Ибо в таких файлах по заявленному способу, есть метки о потенциале вредоносности, и операционная система ключа не даст использовать их возможности для взлома каких-либо файлов или процессов первого уровня защиты.

Вообще, та вольница, которая есть сейчас у пользователя для проникновения в системные файлы операционной системы и изменения их, будет исключена.

В целом, представив полное распространение этого способа защиты по планете, спектр исполняемых файлов 3 категории видится не таким уж и великим для простого пользователя. Имеется в виду полезный, не опасный софт. Другой контент в виде видеофайлов, аудиофайлов, текстовых, графических и иных, не являющихся исполняемыми, опасности представлять не будет.

По сути, законопослушный пользователь даже не заметит особой разницы в работе своего компьютера.

Посему, может оказаться целесообразным полная блокировка работы исполняемых файлов 3 категории. Кроме, разумеется случаев разработки программного обеспечения. Но там исполняемый файл будет находиться в среде программирования, являющейся процессом 1 категории, а это уже совсем другая история.

Сейчас, исходя из логики рассматриваемого способа защиты, надо увидеть:

Как в данный момент действуют угрозы в сфере Информационных Технологий?

Ответ прост: они действуют исходя из свободного доступа к ресурсам хоть чего!

Будь то ресурсы аппаратные: процессор, оперативная память, жесткий диск с его загрузочными секторами и другое.

Будь то ресурсы операционной системы: системные файлы, реестр, да хоть что вообще. Защита же системы строится на хитроумности алгоритмов, которые ломаются другой хитроумностью алгоритмов.

Представленный способ предлагает иное решение. Предлагается поменять среду обитания алгоритмов.

Способы проникновения вредоносного кода в компьютер известны.

Это носители, интернет, закладки в софте, клавиатура.

С носителями, бэкдорами в софте и клавиатурой всё ясно, всё это сразу определяется как 3 категория.

А что же интернет?

Здесь вредоносный код пытается влезть в компьютер «на плечах» законного ПО.

Например, браузер, вполне законная программа 1 категории для выхода в интернет. Даже если в браузере есть какая то уязвимость, то для того чтобы узнать о ней, браузер надо изучить, а это не даст сделать система ключа. Причем ни внутри компьютера, ни при попытке извне. Даже если сам разработчик браузера, знающий об этой уязвимости, попытается её воспользоваться, то его попытки будут процессами 3 категории действующими извне и система ключа их заблокирует.

Здесь всё упирается в скрипты.

Но что они смогут в новой среде обитания алгоритмов?

Попытаться записать на жесткий диск какой-либо файл из сети? Может быть…

Попытаться запустить этот файл? Да. А результат? – 3 категория.

Попытаться изменить запись в реестре? Система ключа не даст.

Попытаться изменить системный файл? Система ключа не даст.

Вредоносный код, который попадает в компьютер пользователя вместе с почтой – будет не опасен, т.к. идентифицируется операционной системой ключа как файл и процесс 3 категории. Стандартное состояние таких компонентов как BIOS, загрузочные сектора жесткого диска и др. также легко контролируются ключом.

Сейчас компьютер не находится под контролем чего-либо. В компьютере просто обитают на одном уровне возможностей разные субъекты. Кто-то защищен сильнее, кто-то нет. Кто-то вообще не защищен. Поэтому скрипты делают что хотят. Процессор это тупо исполняет.

В заявленном же способе за всем следит система ключа, в том числе и за аппаратной составляющей. Процессы отслеживаются с момента их рождения. При этом место рождения и родители, влияют на возможности родившегося процесса.

Надо еще учесть и тот момент, что при внедрении в жизнь этого способа защиты, взломать сайты станет не таким уж и простым делом. Ведь серверы тоже будут работать по принципу этого способа. Поэтому поместить вредоносную ссылку на добросовестном сайте будет не просто, а скорее невозможно. Тогда за вредоносный код несет ответственность владелец сайта.

Теперь о трудностях внедрения в жизнь заявленного способа. Есть ли они?

На первый взгляд основная трудность – это замена оборудования на всей планете у всех пользователей.

Если смотреть на это с точки зрения сиюминутности, вот прямо сейчас и срочно, то, конечно задача кажется вообще не осуществимой.

Если смотреть на это с точки зрения истории и неотвратимости прогресса, то внедрение этого способа в жизнь видится неизбежным.

Какие же стимулы являются ускоряющими реализацию этого способа? Что именно подтолкнёт этот способ к скорейшему внедрению?

На первый план выходит, конечно же, финансовый вопрос.

Какова стоимость внедрения этого способа для внедряющих его?

Итак, первый компонент, который надо заменить в существующем оборудовании – это процессор. Что это будет стоить внедряющим? Ответ – ничего. Ибо затраты на процессор окупаются при его продаже.

Второй компонент – это аппаратный ключ. Но он тоже окупается при его продаже. Равно как и сетевая карта.

Сервер – вот основная затрата людей, осуществляющих способ.

Но сопоставимы ли затраты на создание такого сервера, с прибылями от защиты интеллектуальных прав этим способом?

Сколько будут получать защитники интеллектуальной собственности?

Для этого надо представить, сколько миллиардов копий контента делается в мире за год. Видеофильмы, музыка, игры, софт. **Весь** контент, и пиратский и легальный.

В мире более 3 миллиардов пользователей сети интернет. У каждого может оказаться несколько гаджетов. Как правило, так и есть. Как минимум смартфон и ноутбук. Сколько копий контента делается пользователем в год на все его устройства? Видео, музыка, софт, игры, электронные книги и многое другое.

Даже если представить среднее число в 100 единиц контента в год на пользователя, то получается 300 миллиардов копий. Если с копии брать за защиту хотя бы 10 центов, то стоимость сервера окупится менее чем за год. При этом себестоимость защиты мизерна, а качество высокое.

Все страдающие от пиратов производители контента будут весьма довольны качеством защиты своей продукции, даже если цены за защиту оставить такими, какие они есть сейчас, когда на копию контента делается отдельный аппаратный ключ, который стоит не 10 центов.

Производители видеопродукции только в мечтах видят такое качество защиты одной копии своего товара. Производители аудиопродукции вообще не мечтают ни о чем, они просто страдают. В мире, где царит этот способ, выложить защищаемую музыку в сеть в виде пиратской копии – это, то же самое что просто сдаться полиции. Ну и, разумеется, производители дорогостоящего софта и софта вообще, тоже не прочь защищать свою продукцию с таким качеством.

Можно представить, сколько могут в год получать защитники интеллектуальных прав, используя этот способ.

Более того, в бизнесе есть закон: можешь взять – бери.

Этот способ дает техническую возможность брать с каждого сайта за защиту от взлома. Либо процентом с рекламы, либо фиксированным тарифом.

Как становится видно, прибыль набегает немаленькая, при затратах на создание одного сервера.

Проще всего этот способ осуществлять тем, кто имеет возможность производить современные высокотехнологичные процессоры. Однако может так оказаться, что те, у кого есть право осуществлять заявленный способ, не имеют мощностей для производства современных высокотехнологичных процессоров.

Но захотят ли идти им навстречу те, кто имеет производство процессоров? Думается да. Ведь достаточно представить себе объём продаж нового железа и соответственно прибылей, и всё становится ясно.

Теперь обнаруживается следующий вопрос: а захотят ли пользователи тратить деньги на покупку новых процессоров и ключей? А скорее всего и на покупку новых материнских плат?

Для этого надо осознать, кто от кого зависим. На первый взгляд производители контента зависят от покупателей своей продукции.

Но и пользователь как наркоман зависит от нового контента.

Желая защититься от пиратов, и получать **всю** свою прибыль от вложенных денег, производители контента могут заставить пользователя переходить на новую технологию, выпуская свой контент только под неё. Тут производители контента и производители железа выступают единым фронтом.

Кто в такой ситуации моргнёт первым? Долго ли протянет пользователь без нового контента в условиях, когда в магазине на прилавках новые процессоры, открывающие доступ к новому контенту?

Ведь, по сути, получится, что финансировать внедрение этого способа будут пользователи, в то время как рычаги стимулирующие такое финансирование находятся у получателей прибыли. Захотят ли при таких условиях производители контента и железа надавить на пользователя, чтобы тот профинансировал новый порядок в информационных технологиях, чтобы в итоге производители контента получали всю прибыль за свою продукцию?