«Там на неведанных дорожках, следы невиданных зверей …»

Лирическое отступление о недекларированных возможностях к эссе на тему проектов Постановлений Правительства РФ по защите ПДн

С. В. Вихорев,
Заместитель генерального директора
ОАО «ЭЛВИС-ПЛЮС» по развитию

10-11.10.2012 г.

Как было хорошо раньше! Есть идентификационные ПДн – одна степень защиты, нет - другая. Все просто и понятно. Правда, в начале тоже немного поспорили: что, где и почем. Но потом все встало на свои места. И вдруг, бац! – вторая смена! А все потому, что волею судеб (если, конечно, чиновника считать судьбоносной фигурой), недекларированные (недокументированные!) возможности стали тем самым водоразделом, который по одну сторону оставил обязательное применение сертифицированных средств защиты при обработке ПДн, а по другую – альтернативное решение. Проще говоря, если злоумышленнику есть возможность использовать НДВ в общесистемном и прикладном ПО, то у тебя один тип угроз и высокий уровень защищенности ПДн, а если такой возможности нет – другой тип угроз и низкий уровень защищенности ПДн, который гораздо проще в реализации. По крайней мере, так можно истолковать проекты постановлений Правительства по защите ПДн. Вот он, звездный час неправильного русского слова «НЕДЕКЛАРИРОВАННЫЕ»!

И сразу же в блогах по проблемам безопасности информации разгорелся спор: кто сетует на то, что угрозы, связанные с НДВ актуальны для всех и теперь потребуется использовать сертифицированные на НДВ операционные системы, кто озабочен тем, как доказать, что угрозы, связанные с НДВ не актуальны, кто пытается разобраться, а что такое вообще недекларированные возможности. Вот-вот-вот! Это, наверное, самое главное сейчас. Попробую и я порассуждать на эту тему.

Who is who

Вообще-то, правильнее всего начинать с точного определения того понятия, которое мы рассматриваем. Поэтому обратимся к Марксу (то бишь к первоисточнику). В РД (руководящем документе), определяющем в частности, классификацию ПО средств защиты информации по уровню контроля отсутствия недекларированных возможностей сказано:

> *«2.1. Недекларированные возможности — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности информации».*

Этого же мнения придерживается и ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Так что имея два таких авторитетных источника, мы можем с уверенностью считать такое определение правильным и общепризнанным. Кстати, надо упомянуть и то, что эти РД и ГОСТ выделяют в особый термин – «программные закладки» – преднамеренно (то есть злоумышленно) внесенный в ПО функциональный объект, который при определенных условиях позволяет использовать возможности недекларированных возможностей ПО. И что же это нам дает? Прежде всего то, что НДВ — это функциональные возможности ПО, причем только те, которые не описаны в документации на ПО. А есть ли таковые? Конечно, есть. Например, специальные комбинации клавиш сотовых телефонов, открывающие доступ к инженерным или диагностическим меню (многие ли знают о команде *#06#, которая позволяет получить доступ к идентификационным данным телефона или его конфигурации?). В операционной системе к таким возможностям можно отнести команды, позволяющие работать с реестром или, например, API. Специальная комбинация клавиш или удержание клавиши при включении позволяет производить с принтером недокументированные в инструкции действия, такие как перевод в сервисный режим для диагностики.

К сожалению, очень часто под НДВ понимают уязвимость ПО. Но, на самом деле, это не так. В ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», сказано:

«2.6.4. Уязвимость (информационной системы) – брешь: свойство ИС, обуславливающая возможность реализации угроз безопасности обрабатываемой информации».

Да и в ГОСТ Р ИСО 7498-2-1999 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации» есть аналог:

«Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации».

Получается, что понятие уязвимости гораздо шире, чем понятие НДВ. И самое главное, уязвимость принадлежит системе в целом, а не ПО в частности. Уязвимость может возникнуть в результате ошибок программирования и проектирования информационной системы, использования ненадежных паролей, вирусных атак и применения других вредоносных программ (опять же есть разница между вирусами и вредоносными программами, но об этом как-нибудь в другой раз). Отсюда вывод: НДВ может служить уязвимостью, но не всякая уязвимость (даже в ПО) обусловлена НДВ. Но в проектах постановлений Правительства говорится именно о возможности применения НДВ, как критерии выбора уровня защищенности ПДн. И транспонировать эти определения на все уязвимости – не правильно. Кстати, методы анализа и поиска НДВ сильно отличаются от методов поиска и анализа уязвимостей. К сожалению, пен-тестами НДВ не найти.

Кроме того, функциональные возможности (или просто функциональность ПО), которые, судя по определению, присущи именно НДВ, по ГОСТ 28806-90 «Качество программных средств. Термины и определения» являются совокупностью свойств ПО, определяемых наличием набора функций, способных удовлетворять потребности пользователя. А уязвимость это та «дыра» в ПО, которая позволяет «обмануть» приложение — заставить его совершить действие, на которое у того не должно быть прав (но не функциональных возможностей!).

То есть, говоря по-русски, в приложении есть некая функциональная возможность, которая при определенных условиях (например, наличия программной закладки, позволяющей изменить права пользователя) может быть использована для причинения вреда полезной информации. Но это далеко не НДВ – все функциональные возможности конкретного ПО, как правило описаны (задекларированы), а изменение прав – это не функциональная возможность этого конкретного ПО!

Ну прямо как в известной сказке: «Это сон про не сон…». Попробуем все-таки разобраться со всеми сущностями типа «НДВ», «программные закладки», «вредоносные программы» и определить, где и как они пересекаются и что к чему можно отнести.

Кратко об актуальности НДВ

Не просто продираться сквозь дебри специальных терминов. Сухие строчки стандартов не дают всю гамму красок, рисующих эти определения. Вот если бы к каждому стандарту еще и голову разработчика приложить! А так как чужой головы у нас нет, будем обходиться своей и включим в работу, как говорил Эркюль Пуаро, «серые клеточки».

Для начала уясним, что неправомерные действия с информацией могут совершать либо субъекты (назовем их санкционированными пользователями), имеющие легальный (санкционированный) доступ к информации, но превышающие свои права, либо субъекты (назовем их несанкционированные пользователи), не имеющие легального доступа к информации, но стремящиеся получить такой доступ для достижения своих преступных целей. (Кстати, к преступным можно отнести и желание самовыразиться или потешить свое самолюбие).

И еще, надо понимать, что любые преступные цели могут быть достигнуты как с использованием тех функциональных возможностей (назовем их штатными возможностями ПО), которые уже заложены в ПО при его разработке и служат целям удовлетворения пользователя при использовании такого ПО, так и при помощи дополнительных возможностей (назовем их нештатными возможностями ПО), которые тем или иным способом специально внедрены в ПО и негласно расширяют штатные возможности ПО (например, штатно Adobe Reader позволяет читать файлы в специальном формате, однако в него может быть

внедрен дополнительный программный код, который реализует нештатную возможность запоминать читаемые файлы и пересылать их по определенному адресу).

Правда, для использования в преступных целях штатных возможностей злоумышленнику, по всей вероятности, придется изменить те права, которыми наделен санкционированный пользователь (например, разрешить ему доступ к той области данных, которые в обычной ситуации для него закрыты). В этом случае несанкционированный пользователь как бы маскируется под санкционированного пользователя. С учетом этого попробуем сформулировать несколько типовых ситуаций при которых возможно совершать какие-либо операции с информацией:

Варианты неправомерных действий	**Операции с информацией реализуются:**	**Недекларированные возможности**	**Программные закладки**	**Вредоносные программы**
I вариант	Санкционированным пользователем, превышающим свои права с использованием специально заложенных в ПО технологических возможностей, не декларированных в документации пользователя, но необходимых в процессе эксплуатации ПО			
II вариант	Несанкционированным пользователем с использованием специально заложенных в ПО технологических возможностей не декларированных в документации пользователя, но необходимых в процессе эксплуатации ПО			
III вариант	Несанкционированным пользователем с использованием не устраненных при отладке ПО технологических возможностей не декларированных в документации и не требуемых в процессе эксплуатации ПО			
IV вариант	Несанкционированным пользователем с использованием штатных возможностей ПО в результате случайных ошибок программирования, позволяющих изменять права использования штатных возможностей ПО			
V вариант	Несанкционированным пользователем с использованием штатных возможностей ПО в результате преднамеренных ошибок программирования, позволяющих изменять права использования штатных возможностей ПО			
VI вариант	Несанкционированным пользователем с использованием специально заложенных путем внедрения при программировании в ПО дополнительного программного кода нештатных (дополнительных) возможностей ПО			
VII вариант	Несанкционированным пользователем с использованием специально заложенных путем внедрения при программировании в ПО дополнительного программного кода, позволяющих изменить права использования штатных возможностей ПО			
VIII вариант	Несанкционированным пользователем с использованием полученных в результате введения в ПО в ходе его эксплуатации дополнительного программного кода, реализующего нештатные (дополнительные) возможности ПО			
IX вариант	Несанкционированным пользователем с использованием полученных в результате введения в ПО в ходе его эксплуатации дополнительного программного кода, реализующего возможность изменения права использования штатными возможностями ПО			

Так как нас интересует именно НДВ, в дальнейшем будем рассматривать только первые 5 вариантов неправомерных действий. Если внимательно присмотреться, можно увидеть, что для любого случая злоумышленнику по крайней мере надо знать о тех нендекларированных возможностях, которые есть в ПО. Как это возможно? Можно самому проанализировать программный код, но это не каждый сможет: время анализа сопоставимо с временем разработки кода. А времени у санкционированного пользователя, как ни странно, нет. Можно воспользоваться плодами специалистов, которые это умеют делать быстрее и имеют для этого специальные инструменты, но, как правило, такие специалисты сидят в закрытых лабораториях и не каждому готовы дать результаты своих исследований. Можно еще обратиться к разработчику ПО, что бы он подсказал, где эти самые НДВ лежат, но вряд ли он сам об этом расскажет. Получается, что злоумышленнику для того чтобы воспользоваться НДВ надо либо иметь высокую квалификацию, либо иметь доступ к закрытым источникам. Да еще надо обладать некоторыми не слабыми познаниями в программировании, чтобы незаметно использовать то, что заложено в ПО.

Ага! Вот она где собака зарыта! Получается, что сами по себе НДВ – это лишь верхушка кораллового рифа, создающего легкие бурунчики на глади моря. Но зиждется этот риф на твердой основе тектонических пород из квалификации и возможностей злоумышленника. То есть говоря о НДВ, мы имеем ввиду квалификацию и возможности злоумышленника.

Тогда I вариант неправомерных действий возможен, если в штате организации имеется «засланный казачок», получивший специальное образование и практику анализа программного кода, да еще и легально допущенный к некоторой информации. Но такой специалист дорог. А не проще ли ему просто-напросто в дружеской беседе за рюмкой чая со своим «другом», который допущен к нужной информации, попытаться узнать пароли доступа, коды, а может быть и саму информацию. С этой задачей справится и «инженер человеческих душ», даже не имея специального образования. Наверное, I вариант действия злоумышленника возможен, если в организации действительно есть очень-очень важная информация о важной персоне и, к тому же, хорошо работает служба безопасности. Так что вариант реальный, но маловероятный.

Остальные 4 варианта предполагают, что действия совершает несанкционированный пользователь. А такой пользователь может быть как внутри самой организации, так и за ее пределами. Правда, если злоумышленник находится внутри организации, то применимы рассуждения, приведенные выше: мы просто имеем вырожденный случай I варианта. Поэтому, логичнее рассматривать случай, когда злоумышленник находится за пределами организации. Такой «хакер», конечно, имеет время для подготовки и предварительного анализа программного кода для выявления НДВ, да и, при необходимости, он может подключить для этих целей серьезные научные организации (если, конечно, ожидаемая информация того стоит), но он имеет гораздо меньшие возможности для проникновения в саму информационную систему. То есть такому злоумышленнику надо решить сразу две задачи: найти способ как проникнуть в ИС и найти способ как воспользоваться НДВ. Сразу же встает вопрос: а не проще ли в этом случае не искать НДВ, а сразу внедрить какую-то утилиту, которая позволит получить требуемую информацию? Но это уже получается VI – VIII варианты действий, а они связаны с программными закладками, но не с НДВ.

Особо хочется остановиться на IV и V вариантах. IV вариант предполагает поиск случайных ошибок программирования. Действительно, в мире нет ПО, свободного от ошибок! Это аксиома. Но найти случайные ошибки, которые позволяют изменить права пользователя – дело весьма сложное, можно даже сказать случайное. V вариант – пограничный. Для его реализации надо иметь не только злоумышленника, который будет использовать некую ошибку программирования, но еще надо иметь того самого программиста, который специальным образом, то бишь преднамеренно, внесет такую ошибку при составлении программного кода (трудно понять это действительно НДВ или уже программная закладка). То есть реализация такого варианта в два раза дороже, чем остальных.

Правда, надо сказать, что использовать возможности НДВ «в слепую» («давайте что-нибудь получим, а потом посмотрим нужно ли это нам») вряд ли кто-то будет. Использовать такой механизм добывания информации в силу сложности его реализации будут в случае, если надо получить какие-то конкретные ПДн о каком-то конкретном субъекте. В противном случае это экономически не оправдано. По всей вероятности, рейтинг злоумышленников, при условии, что добываемая информация действительно представляет для них ценность, и они пытаются получить именно эту конкретную информацию, может выглядеть так:

- ✓ I вариант действий – средний уровень квалификации, средний уровень осведомленности о наличии НДВ, высокая степень заинтересованности в получении конкретных ПДн о конкретном субъекте;
- ✓ II вариант действий – средний уровень квалификации, средний уровень осведомленности о наличии НДВ, средняя степень заинтересованности в получении конкретных ПДн о конкретном субъекте;
- ✓ III вариант действий – высокий уровень квалификации, высоки уровень осведомленности о наличии НДВ, очень высокая степень заинтересованности в получении конкретных ПДн о конкретном субъекте;
- ✓ IV вариант действий – очень высокий уровень квалификации, высоки уровень осведомленности о наличии НДВ, очень высокая степень заинтересованности в получении конкретных ПДн о конкретном субъекте;
- ✓ V вариант действий – очень высокий уровень квалификации, очень высокий уровень осведомленности о наличии НДВ, очень высокая степень заинтересованности в получении конкретных ПДн о конкретном субъекте.

В завершении хочу дать совет: для оценки актуальности угроз, которые могут быть реализованы с использованием возможностей НДВ, прежде всего надо оценивать важность самой информации, а так же

квалификацию и возможности злоумышленника. Для этого предлагаю пользоваться классификацией, приведенной в предыдущем абзаце. И уже с учетом данного рейтинга, принимать необходимые и достаточные меры для защиты своих данных. Однако, прекрасно понимаю, что совет как касторка: легко давать, но сложно принимать.