Сертификация средств защиты персональных данных: революция или эволюция?

А. Марков,
М. Никулин,
В. Цирлов

ЗАО «НПО «Эшелон»
www.npo-echelon.ru

Актуальность

Вступление в силу ФЗ-152 «О персональных данных» взволновало ИТ-сообщество тем, что миллионы российских информационных систем, касающихся сбора персональных данных (ПДн), должны быть приведены в строгое соответствие с совершенно новыми требованиями, причем приведены уже к концу следующего года!

Эти требования в текущем году сформулированы в совместном Приказе ФСТЭК России, ФСБ России и Мининформсвязи России, а также нормативных документах ФСТЭК России и ФСБ России. В чем же их особенность? Во-первых, требования к системам приобрели статус обязательных для любых организаций, независимо от формы собственности последних. Во-вторых, требования в ряде случаев стали более жесткими, чем ранее практикуемые при защите конфиденциальной информации. В-третьих, требования сформулированы для новых сервисов, средств и мер защиты. И последнее: нормативные документы только начали апробацию.

Важным моментом обеспечения безопасности ПДн является требование Постановления Правительства РФ 2008 года № 781 по обязательности *оценки соответствия* средств защиты ПДн, которая в настоящее время выражается в такой ответственной и длительной процедуре как сертификация.

Обычно потребители сертифицированной продукции задаются рядом вопросов: так ли уж обязательна сертификация, что грозит за нарушения процедуры, как оптимизировать процесс, что ожидать в ближайшем будущем? Эти вопросы с точки зрения испытательной лаборатории и будут рассмотрены в статье.

Системы и объекты сертификации персональных данных

Сертификация по требованиям безопасности информации представляет собой деятельность по подтверждению характеристик продукта, услуги или системы требованиям стандартов или иных нормативных документов по защите информации. В нашей стране действуют четыре федеральных органа по сертификации, однако в области защиты ПДн сферы ответственности поделены между ФСБ России и ФСТЭК России. Традиционно сфера компетенции ФСБ России лежит в области криптографической защиты, а сфера ФСТЭК России – в области некриптографической защиты информации от несанкционированного доступа, а также от утечек по техническим каналам связи. Тем не менее, чтение документов показывает, что возможно расширение деятельности по линии ФСБ России, в частности, это очевидно для систем обнаружения вторжений (IDS).

Сертификации подлежат системы, продукты и услуги. В рамках

систем обязательной сертификации мы имеем дело с первыми двумя. Например, в руководящих документах Гостехкомиссии России продуктом может выступать средство вычислительной техники (СВТ), средство защиты информации (СЗИ), межсетевой экран (МЭ), программное обеспечение (ПО) и др. Система – это объект информатизации, где обрабатывается реальная информация. По этой причине к системам предъявляются дополнительные требования, касающиеся, в том числе, организационных мер и физической защиты.

Информационные системы ПДн (ИСПДн) поделены на 4 класса по степени возможных последствий для субъектов ПДн вследствие возникновения инцидентов в этих системах: К1 (значительные последствия), К2 (последствия), К3 (незначительные последствия), К4 (не приводят к последствиям). Класс типовой ИСПДн можно определить в соответствии с табл. 1.

ИСПДн также разделяют:

- по наличию подключения к сетям общего доступа (с подключением или без);
- по правам пользователей (однопользовательские, многопользовательские с равными правами пользователей, многопользовательские с различными правами пользователей).

СЗИ, используемые в ИСПДн, выбираются с учетом актуальных угроз системе и декларируются в схеме деления системы.

В нормативных документах по ПДн в качестве обязательных определены следующие СЗИ:

- средства предотвращения несанкционированного доступа;
- средства защиты информации при межсетевом взаимодействии;
- антивирусные средства;
- средства анализа защищенности;
- средства обнаружения вторжений;
- криптографические средства.

Кроме того, по тексту упомянуты обманные системы и средства «горячего» резервирования. По сравнению с документами Гостехкомиссии России по СВТ функционал средств защиты от несанкционированного доступа к информации также существенно расширен. В явном виде не определен ряд современных средств и сервисов (например, средства аутентификации II и III типов, генерации и управления паролями, багтрекинга и другие), однако они могут быть добавлены с учетом разработанной модели угроз.

Таблица 1. ***Классификация информационных систем персональных данных***

Число субъектов ПДн (объединение) / Категория ПДн	Менее 1000 (организация)	1000-100000 (город)	Более 100 000 (субъект федерации)
Обезличенные ПДн	К4	К4	К4
ФИО, адрес, день рождения	К3	К3	К2
Образование, финансы	К3	К2	К1
Здоровье, любовь	К1	К1	К1

Таблица 2. ***Условия применения только сертифицированных средств защиты***

Категория информации	Государственная тайна	Конфиденциальная информация	Открытая общедоступная
Государственный информационный ресурс	Всегда	Всегда	При доступе из международных сетей общего пользования
Негосударственный информационный ресурс	–	• В АСУ экологически опасных производств, ключевых систем, критически важных объектов, потенциально опасных объектов инфраструктуры РФ • В игровых автоматах (на отсутствие недекларированных возможностей (НДВ) • На аттестованных объектах информатизации • При защите персональных данных	Не проводится

Напомним, что по линии ФСТЭК России требования, сформулированные в виде отдельных руководящих документов, имеются только для комплексных средств защиты от несанкционированного доступа к информации и для МЭ.

Требование по обязательности сертификации

Если нормативные документы ФСБ России выполнены в традиционном для документов по криптографической защиты конфиденциальной информации стиле, то нормативные документы ФСТЭК России имеют в некотором роде революционный характер. В первую очередь это связано с декларированием обязательности сертификации средств защиты как государственного, так и негосударственного информационного ресурса (табл. 2), а также с обязательными условиями сертификации, выразившимися в лицензировании эксплуатации ИСПДн.

Так, в п. 5 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» указано, что СЗИ, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Установленный порядок назначается уполномоченными органами, в данном случае ФСТЭК России и ФСБ России. Согласно документам ФСТЭК России *все СЗИ, используемые в ИСПДн, проходят сертификацию на соответствие требованиям по безопасности информации.*

Принципиальным моментом является то, что *программное обеспечение* СЗИ от угроз конфиденциальности, целостности и доступности подлежит сертификации на отсутствие *недекларированных функциональных возможностей.* Такая позиция федеральных органов совершенно понятна, так как очевидно, что уязви-

мости ПО представляют самое слабое звено любого ИТ-проекта. Данный пункт имеет особое значение, поскольку его соблюдение влечет обязательное предоставление исходных текстов на программный код средств защиты.

Что касается автоматизированных систем, то текущая версия нормативных документов подразумевает обязательную сертификацию и/или аттестацию ИСПДн класса 1 и 2. Для ИСПДн 3 класса возможна декларация соответствия, то есть протоколы сертификационных испытаний может подготовить сам разработчик, однако последнее слово все равно остается за федеральным органом. Следует указать, что если заявитель пожелает только аттестовать ИСПДн как объект информатизации, то пока действуют традиционные нормативные требования по аттестации объектов информатизации (СТР-К), в которых обрабатывается конфиденциальная информация.

Требования по обязательной сертификации систем и средств однозначно определены на всех этапах создания ИСПДн. При задании требований к системе в ТЗ и ЧТЗ уже должен быть представлен перечень предполагаемых сертифицированных СЗИ, на этапах реализации проекта производится внедрение сертифицированных средств или инициируется сертификация несертифицированных решений, а на этапе ввода в действие осуществляется оценка соответствия всей системы этим требованиям.

Новым дискутируемым условием эксплуатации ИСПДн 1 и 2 класса, а также распределенных ИСПДн 3 класса является наличие лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации. Следует отметить, что оператор или разработчик, пожелавший инициировать сертификацию систем и средств ПДн должен еще иметь лицензию на разработку СЗИ. Аналогичные подвиды деятельности по линии ФСБ России тоже подлежат лицензированию. Следует понимать, что с учетом 7 миллионов операторов, процесс лицензирования может приобрести для страны мобилизационный характер.

Кого накажут?

Безопасность – область социальная, и с учетом человеческого фактора и стремительно развивающихся информационных технологий, конечно, не может быть абсолютной. Инциденты и нарушения будут существовать вечно. В такой ситуации важно найти тех, кто понесет ответственность по всей строгости в случае утечки или утраты ПДн.

Еще в ФЗ-1 «Об электронной цифровой подписи» было указано, что возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами, может быть возложено на *создателей и распространителей* этих средств.

В ФЗ-152 «О персональных данных» основным ответственным лицом определен *оператор* – госорган, юридическое или физическое лицо, организующее обработку ПДн. Так, в ст. 19 ФЗ-152 отмечается, что оператор обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерных действий. С учетом особенностей получения лицензии по защите информации ответственность ляжет на юридические лица и их руководство.

В «Положении об обеспечении безопасности персональных данных…» в п.п. 10 и 17 отмечается, что на основании договора можно переложить часть ответственности при обработке ПДн на так называемое *уполномоченное лицо*, а при разработке ИСПДн и СЗИ – собственно на *разработчика*.

Преступление и наказание

Ст. 24 ФЗ-152 «О персональных данных» гласит, что лица, виновные в нарушении требований Федерального закона, несут гражданскую, *уголовную*, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Ответственность за нарушения требований обязательной сертификации в явном виде определена в КоАП. Так, в ст. 13.2 п. 2 говорится: «Использование несертифицированных СЗИ (за исключением средств защиты информации, составляющей государственную тайну) влечет наложение административного штрафа на юридических лиц – от 100 до 200 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой, на должностных лиц – от 10 до 20 МРОТ[1]». К концу следующего года оператор персональных данных должен определиться: конфискация или сертификация.

Кроме того, нарушителей правил и условий использования ИСПДн можно классифицировать по ст. 13.2, 13.13 и 13.14 КоАП. Нарушения такого рода приведут к отзыву лицензии и конфискации оборудования. По утверждению Россвязькомнадзора, в самое ближайшее время ожидается развитие ст. 13 КоАП в сторону уточнения нарушений при обработке ПДн.

Появление ФЗ-184 «О техническом регулировании» отменило ряд законов, которые предусматривали уголовную ответственность за использование несертифицированных средств. Однако это не означает, что игнорирование обязательной сертификации пройдет безнаказанно. В ст. 171 УК РФ установлено наказание за нарушение лицензионных требований и условий (конечно, распространяемых и на использование сертифицированных СЗИ) *сроком* до 6 месяцев. Следует указать, что в УК РФ содержится около десяти глав, где статьи касаются деяний, при совершении которых нарушитель может использовать системы обработки и защиты идентификационной информации в разных сферах жизни, будь то военная служба, правосудие, компьютерная сфера, экономическая деятельность или конституционные права. Как правило, это – разглашение, халатность, нарушение правил, злоупотребление при ор-

[1] *МРОТ - 2300 руб. с 01.09.07.*

ганизации работ по созданию и эксплуатации информационных систем.

Любопытно сравнить ситуацию, сложившуюся в области защиты ПДн за рубежом. Ярким примером является американский закон Health Insurance Portability and Accountability Act, Public Law 104-191 (HIPAA). Все организации, где имеется информация, *касающаяся здоровья граждан*, обязаны обеспечивать ее безопасность. Требования административного, физического и программно-технического характера сформулированы в документе HIPAA Security Rule. Нарушителям закона грозит тюремный срок до 10 лет.

В заключении добавим, что в Россвязькомнадзоре уже сформирован план проверок выполнения требований ФЗ-152 на год.

Нормативные требования к средствам защиты персональных данных

Просматривая сертификат, важно обратить внимание, на соответствие каким документам проведены сертификационные испытания.

Что касаемо ФСТЭК России, то это может быть:

- руководящие документы Гостехкомиссии России по защите от несанкционированного доступа к информации (для АС, СВТ или МЭ);
- руководящий документ Гостехкомиссии России по контролю отсутствия недекларированных возможностей;
- техническое условие или формуляр;
- задание по безопасности (по требованиям ГОСТ ИСО/МЭК 15408-2002).

Так как руководящие документы существуют не для всех классов СЗИ, требования, указанные в нормативных документах по ПДн, придется вписывать в ТУ или в задание по безопасности (ЗБ). Напомним, что руководящие документы Гостехкомиссии России представлены на официальном сайте www.fstec.ru в свободном доступе. Нормативные документы ФСБ России могут получить только соответствующие лицензиаты. Четыре последних нормативных документа ФСТЭК России по ПДн носят служебный характер, но распространяются лицензиатам *с правом их тиражирования*. Непосредственных потребителей этих документов – около 7 миллионов операторов ПДн, то есть конфиденциальность их будет соблюдена в узком кругу 7 миллионов юридических лиц или, по приблизительным оценкам, 142 миллионов человек.

Поскольку руководящие документы, на соответствие которым следует проводить сертификационные испытания именно ИСПДн, не сформированы, процедуры сертификации и аттестации систем и средств ПДн не претерпели каких-либо изменений по сравнению с действующими.

Следует разобраться, какими сертификатами на СЗИ должны обладать ИСПДн каждого класса с учетом их категории и применения.

Классы средств защиты персональных данных

Рекомендации и требования («Основные мероприятия..») включены в нормативные документы ФСТЭК России. В рекомендательной части по тексту встречаются указания для двух классов СЗИ, а именно, МЭ и IDS (табл. 3).

Таблица 3. ***Рекомендации по использованию средств защиты в ИСПДн***

Класс ИСПДн	Класс МЭ	Типы IDS
К1	3	Сигнатурные и аномальные
К2	4	Сигнатурные и аномальные
К3	5	Сигнатурные
К4	5	Сигнатурные

Таким образом, в ИСПДн 1 класса рекомендованы к применению МЭ, предназначенные для межсегментной или межсетевой защиты сетей, где обрабатываются сведения, содержащие государственную тайну. При сертификации IDS-систем указанные требования должны быть вписаны в ТУ или ЗБ.

Если внимательно изучить текущую версию документа по требованиям к средствам защиты ПДн, то можно заметить очевидную корреляцию (совпадение клеше текстов) с руководящими документами Гостехкомиссии России по защите информации от несанкционированного доступа для АС и для МЭ. Это сделано совершенно логично для соблюдения приверженности всем апробированным нормативным наработкам. Указанные совпадения с руководящими документами Гостехкомиссии Российской Федерации представлены в табл. 4.

Какие требования к ИСПДн имеют корреляцию с требованиями к системам, ориентированным на защиту информации, составляющей государственную тайну? Это АС класса 3А, 2А, 1В и МЭ класса 2 и 3.

Если сравнить таблицы 1 и 4, проясняется содержание сертификатов по средствам защиты ПДн. Например, для реальных АРМ или изолированных ЛВС в системе здравоохранения (К1) должны быть установлены СЗИ, сертифицированные по классу защиты для СВТ не ниже 4, в том числе по уровню отсутствия недекларированных возможностей, видимо, тоже не ниже 4 уровня. При обработке финансовой отчетности на компьютерах отдельной организации (К3) или в изолированной ЛВС муниципального образования (К2) удастся обойтись традиционными сертифицированными средствами защиты конфиденциальной информации (СВТ-5, НДВ-4).

Можно заметить разницу в отношении рекомендаций (табл. 3) и требований (табл. 4) по организации межсетевой защиты при обработке ПДн. В этом случае оператору ПДн следует внимать классику («строгость российских законов смягчается необязательностью их выполнения»), и полагаться на лояльность регулятора.

Итак, что же делать с требованиями, предъявляемыми нормативными документами ФСТЭК России по ПДн, которые не совпадают с требованиями руководящих документов Гостехкомиссии России? Они должны быть описаны в ТУ или ЗБ. Таким образом, все средства защиты ПДн должны быть сертифицированы и на соответствие руководящим документам Гостехкомиссии России, и на соответствие ТУ (или ЗБ).

Таблица 4. ***Корреляция требований к средствам защиты в ИСПДн с документами по АС и МЭ***

Класс ИСПДн	Класс АС	Класс МЭ	
		без подключения к СОД	с подключением к СОД
К1, однопользовательская	3А		2
К1, многопользовательская с одинаковыми правами	2А	4	2
К1, многопользовательская с разными правами	1В	4	2
К2, однопользовательская	3Б+		3
К2, многопользовательская с одинаковыми правами	2Б+	4	2
К2, многопользовательская с разными правами	1Г	4	2
К3, однопользовательская	3Б		4
К3, многопользовательская с одинаковыми правами	2Б	4	2
К3, многопользовательская с разными правами	1Д	4	2
К4	Определяется оператором		

Таблица 5. ***Число сертификаций с 2002 по 2008 годы (сентябрь)***

Системы сертификации	Сертификация по национальным критериям	Сертификация по «Общим критериям»
Минобороны России	540 (756)	3 (экспериментально)
ФСТЭК России: • *продукты, системы* • *профили защиты*	1454 (1835) –	44 3
ФСБ России	Менее 1000	
Международная система Common Criteria (ISO 15408)		
Продукты	–	944
Профили защиты	–	129
FIPS	1021	н/д

В любом случае, в процессе аттестации ИСПДн потребуется творческий процесс оценки содержания сертификатов СЗИ.

Возможные пути развития нормативно-методической базы

Указанные документы, прошедшие первую итерацию, сейчас находятся под пристальным вниманием большого количества специалистов. Очевидно, в них, как это принято в мировой практике, последуют какие-то изменения и доработки. Отметим возможные пути совершенствования нормативно-методической базы ПДн с точки зрения испытательной лаборатории, а именно:

- развитие нормативной базы по линии «Общих критериев»;
- интеграция с национальной системой сертификации систем менеджмента информационной безопасности (СМИБ);
- совершенствование методов выявления НДВ.

Развитие нормативной базы по линии «Общих критериев»

С 2004 года в стране вступил в действие ГОСТ ИСО/МЭК 15408-2002, который получил развитие в руководящих документах Гостехкомиссии России. Технический комитет ТК-362 проводит апробирование проектов новых стандартов по линии «Общих критериев», например: ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО/МЭК ТО 15446, ГОСТ Р ИСО/МЭК ТО 19791 и др. ФСТЭК России подготовлен ряд проектов профилей защиты (ПЗ) и даже три из них сертифицированы. Однако внедрение нормативной базы «Общих критериев» встречает в настоящее время существенную критику со стороны практиков информационной безопасности. Это связано со сложностью понимания стандартов, отсутствием сети специалистов в данной области, длительностью испытаний и неоднозначностью толкования сертификатов при аттестации объектов. При всем этом в стране отсутствует подобный аппарат формализации всеобъемлющих требований к системам и средствам в защищенном исполнении. Думается, проблему подготовки нормативных документов по ПДн можно было решить сертификацией упрощенного для понимания ПЗ.

За рубежом процесс перехода к ОК постепенно набирает обороты, видимо, этот процесс необратим. В табл. 5 проиллюстрирована статистика в различных системах сертификации.

Напрашивается вывод, что при условии продолжения нашей технологической интеграции в мировую индустрию развитие этого направления неизбежно. Направление должно двигаться:

- по пути снижения структурной сложности ПЗ и ЗБ, а, следовательно, затрат;
- по пути повсеместного развития лабораторий и центров компетенции, то есть исключения каких-либо монопольных толкований.

Интеграция с национальной системой сертификации систем менеджмента информационной безопасности

Прошлый год ознаменовался появлением организационных стандартов информационной безопасности по линии ИСО 27000-й серии. Стандарты ввели рекомендации по построению систем информационной безопасности и требования к СМИБ.

В философском плане прослеживается концептуальная связь подходов ИСО 27000-й серии и документов по ДНн: от угроз и рисков – к формированию требований и рекомендаций. Поэтому совершенствование

документов по ПДн в направлении организационных международных стандартов по информационной безопасности позволит использовать наиболее хорошо зарекомендовавшие себя международные практики.

С другой стороны, проведение лицензирования в области создания СЗИ и проверки производств СЗИ (аттестации серийного производства сертифицированной продукции) касаются проверки внедренной в организации системы менеджмента качества. Аудит и сертификация систем менеджмента качества осуществляется по традиции органами систем добровольной сертификации по линии качества, которые подтверждают соответствие организации ГОСТ 9001, ГОСТ 15.002 и др. Указанные проверки ничего общего с системами информационной безопасности не имеют. Следует сказать, что сейчас принята международная система сертификации СМИБ. На сентябрь 2008 года в мире проведено 4803 сертификации, в том числе 10 – в нашей стране. Однако совершенно очевидно, что международная сертификация несопоставима с отечественной ни по стоимости, ни по времени. Поэтому назрела потребность развития национальной системы сертификации СМИБ по линии ИСО 27000-й серии взамен сертификации систем качества по линии ИСО 9000, применительно к организациям-разработчикам СЗИ.

Совершенствование методов выявления недекларированных возможностей

Выявление НДВ проходит красной нитью через несколько документов ФСТЭК России по ПДн. Это связано с тем, что именно ПО является самым уязвимым техническим звеном любой системы. Наличие уязвимостей в ПО служит главной причиной возможных сетевых атак и вирусных эпидемий.

Все существующие системы сертификации в нашей стране придерживаются концепции, выраженной в руководящем документе Гостехкомиссии России по выявлению НДВ. Основной смысл документа заключается в полномаршрутном анализе программного кода. К сожалению, на практике полномаршрутное тестирование относительно сложного продукта невозможно. Выявление НДВ в средствах защиты конфиденциальной информации (4 уровень контроля) принципиально упрощено и касается аспектов исключительно целостности и избыточности ПО. Документ фактически не затрагивает вопросы безопасности ПО, а именно, наличия в нем каких-либо уязвимостей или закладок.

Сейчас накоплен отечественный и зарубежный опыт проведения аудита безопасности программного кода, известного как технология security code reviews. Данная технология ориентирована на выявление уязвимостей кода, влияющих на безопасность. Как это выполняется? Вначале проводится автоматизированный поиск потенциально опасных фрагментов. Следующим этапом выполняется инспекция потенциально опасных фрагментов на предмет некорректностей кодирования (например, переполнения буфера), оставленных паролей, логических бомб и др. После этого проводится анализ на предмет возможности реализации уязвимости злоумышленником (может уязвимость стать угрозой или нет). По результатам аудита выдаются рекомендации по использованию или доработке ПО. Опыт показывает, что потенциально опасных фрагментов в программном коде не более 5–10 %, то есть трудоемкость сертификации может быть снижена. С другой стороны, все закладки и критические уязвимости ПО, с которыми столкнулись авторы в процессе сертификационных испытаний, были выявлены только с помощью такого подхода.

К достоинствам указанного подхода следует отнести его поддержку международными объединениями (QWASP) и то, что он придерживается международной классификации уязвимостей программного кода (CWE).

Выводы

Текущий год показал, что в короткие сроки в стране подготовлен новый и весьма сложный комплект нормативных документов по защите ПДн (в первую очередь имеются в виду документы ФСТЭК России). Данный комплект имеет некоторую преемственность как с традиционными руководящими документами Гостехкомиссии России, так и с международной практикой «от анализа рисков к требованиям и рекомендациям», однако имеет ряд сложных и неоднозначных нововведений. Воплощение требований и рекомендаций документов в жизнь и их апробация только начались, но следует сделать ряд выводов, касающихся сертификации средств и систем защиты ПДн.

1. Средства защиты ПДн подлежат обязательной сертификации независимо от формы собственности организации.

2. В нормативных документах по ПДн отражены тенденции развития информационных технологий, задекларированы новые сервисы, механизмы и средства защиты. Так как в настоящее время отсутствуют универсальные СЗИ, удовлетворяющие указанным требованиям, ожидается развитие существующего рынка разработок в области информационной безопасности.

3. Однозначное требование к выявлению НДВ в ПО потребует от разработчиков предоставления исходного программного кода в рамках сертификационных испытаний. Это может оттеснить с рынка ряд зарубежных МЭ, антивирусов и IDS.

4. Разработчики ИСПДн будут работать с двумя, а с учетом IDS-систем, возможно, даже с тремя обязательными системами сертификации средств защиты по требованиям безопасности информации.

5. Развитие нормативной и методической базы защиты ПДн возможно в направлении:

- разработки и сертификации несложных ПЗ по средствам защиты ПДн, а также развития услуг по линии «Общих критериев»;
- конвергенции организационных мероприятий по защите ПДн со стандартами ИСО 27000-й серии;
- использования отечественного и международного опыта аудита безопасности программного кода при выявлении НДВ. ■