Майор А. В. ФЕДОРЦОВ,
научный сотрудник
Научно-исследовательского института
Вооруженных Сил Республики Беларусь

Полковник Л. Л. УТИН,
начальник кафедры связи военного
факультета Белорусского государственного
университета информатики
и радиоэлектроники,
кандидат технических наук, доцент

МЕТОДИЧЕСКИЙ ПОДХОД К ОСУЩЕСТВЛЕНИЮ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Информационные системы (ИС) и встроенные в них системы защиты информации (СЗИ) представляют собой разнообразную и весьма сложную совокупность программных и технических средств (объектов информатизации (ОИ), систем обработки информации и др.), обеспечивающих осуществление информационных отношений с помощью информационных технологий [1–3]. Все эти взаимосвязанные средства решают огромный круг задач в различных областях человеческой деятельности, а также в военной сфере. Органы и исполнители, осуществляющие контроль за соблюдением требований по защите циркулирующей в ИС информации, сталкиваются с проблемами, связанными, в том числе, с необходимостью своевременного обнаружения и пресечения нерегламентируемой деятельности пользователей, получивших доступ к ОИ и пользующихся ими. Авторами предложен подход, позволяющий частично устранить отдельные проблемы контроля.

УДК 004.056

Согласно нормативным правовым актам (НПА) республиканского уровня [1, 2] в ИС для обработки информации, распространение и (или) предоставление которой ограничено, создается СЗИ. Она представляет собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованную и функционирующую по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Важная роль отводится оператору (владельцу, собственнику), осуществляющему эксплуатацию ИС. В [1] ему предписано, среди прочих обязанностей, обеспечить защиту информации, а также постоянный контроль за соблюдением требований по ее защите.

То есть неотъемлемой функцией оператора является такое управление СЗИ, при котором обеспечивается защита информации, а также постоянный контроль за соблюдением требований по защите информации в ИС. Существенное влияние на эффективность защиты информации при этом оказывает качество контроля.

В руководящих документах Вооруженных Сил Республики Беларусь (далее — ВС) под контролем понимается целенаправленная деятельность соответствующих подразделений (должностных лиц) по выявлению фактического состояния защиты информации в ходе повседневной жизнедеятельности органов военного управления.

На качество контроля в ВС влияют следующие основные факторы:

уровень профессиональной подготовки в области информационных технологий и защиты информации у должностных лиц, привлекаемых для проведения указанных работ;

время, выделяемое на проведение проверки ОИ;

наличие или отсутствие методических указаний и порядка (алгоритмов) действий должностных лиц при проверке ОИ, специализированных компьютерных программ, позволяющих выявлять нерегламентируемую деятельность пользователей.

На практике при осуществлении контроля за соблюдением требований по защите информации возникает ряд проблем, основными из которых являются:

отсутствие методического аппарата по осуществлению процедуры контроля;

низкая оснащенность подразделений по защите информации необходимыми программно-техническими средствами;

привлечение к контролю нештатных специалистов, которые, как правило, не имеют достаточных навыков и опыта.

Указанные проблемы и факторы в совокупности снижают

оперативность обнаружения фактов нерегламентируемой деятельности допущенных к работе на ОИ пользователей, заключающейся в установке и (или) использовании ими компьютерных программ с нарушением установленных правил и полномочий. Все это, в свою очередь, способствует повышению потенциальной опасности утечки информации, распространение и (или) предоставление которой ограничено. Положение усугубляется тем, что на текущем этапе в ВС, несмотря на проделанную огромную работу по развитию корпоративной информационной сети и созданию сетей терминальной архитектуры, все еще эксплуатируется достаточно большое количество автономных ОИ. К тому же современные машинные носители информации (МНИ) выпускаются в форм-факторе различных предметов, и нештатному специалисту, осуществляющему контроль, без соответствующего методического обеспечения выявить факт наличия незарегистрированного МНИ на рабочем месте пользователя (рисунок 1) может быть затруднительно.

Рисунок 1. — МНИ, корпус которого выполняет функции канцелярского предмета

С целью частичного устранения названных проблем была разработана методика обнаружения нерегламентируемой деятельности пользователей на автономных ОИ [4]. При ее разработке учитывалась необходимость комплексного решения существующих проблем. Использование данной методики будет способствовать более качественной проверке проведенных на ОИ мероприятий по заданным направлениям контроля, снижению ресурсоемкости (временных затрат, количества участвующих в контроле специалистов и т. д.), повышению оперативности в представлении результатов (отчетов, анализов и т. д.) и своевременном реагировании на возникшие инциденты (угрозы) для ИС, принятию адекватных управленческих решений. Используемые или разрабатываемые в соответствии с методикой программно-технические средства, в свою очередь, призваны снизить влияние человеческого фактора на полученные данные и расширить границы контроля. В целом вышеуказанные положения являются основой для подготовки специалистов подразделений по защите информации.

Органы и исполнители, осуществляющие контроль за соблюдением требований по защите информации на ОИ ВС, как правило, руководствовались в своей деятельности различными внутренними инструкциями и указаниями, описывающими отдельные стороны контроля. Вместе с тем общие структура и содержание методики контроля до настоящего времени в явном виде не были сформулированы.

Исходя из вышеуказанного, с целью решения основной задачи поиска и обнаружения следов нерегламентируемой деятельности пользователей на ОИ при разработке методики были выделены следующие частные задачи:

определить исходные данные, необходимые для обнаружения нерегламентируемой деятельности пользователей на ОИ;

установить порядок выбора соответствующего метода обнаружения;

определить допущения и ограничения, в рамках которых возможно применение методики;

обосновать основные этапы проверки ОИ;

разработать алгоритм обнаружения нерегламентируемой деятельности пользователей;

разработать формы представления отчетов о результатах проверки ОИ;

разработать рекомендации по применению методики для проведения проверки ОИ.

Установившаяся на практике в ВС периодичность проверки является основным классификационным признаком контроля за деятельностью пользователей на ОИ и находит свое отражение в наименованиях форм проверки:

периодический контроль (плановая проверка использования ОИ);

внезапный контроль (проверка отдельных вопросов защиты информации на ОИ);

постоянный контроль (проверка использования ОИ в ходе повседневной деятельности);

повторный контроль (проверка наличия выявленных в ходе иных видов контроля недостатков (нарушений), реализации предложений и рекомендаций по исключению их проявления в дальнейшем).

Вместе с тем для исключения ситуаций, когда не в полной мере проверяются отдельные аспекты деятельности пользователей и в результате создаются предпосылки к нарушению безопасности информации, была введена дополнительная классификация, раскрывающая глубину проверки:

углубленная проверка (осуществляется только с привлечением специалистов по расследованию преступлений в сфере высоких технологий, когда ОИ стал объектом совершенного преступления либо использовался для его совершения);

тщательная проверка (проводится для обнаружения большего количества фактов нерегламентируемой деятельности пользователя ОИ, а также попыток сокрытия им следов своей деятельности);

быстрая проверка (осуществляется с профилактическими целями и для контроля за деятельностью пользователя ОИ);

поверхностная проверка (используется для своевременного выявления фактов хищения блоков, устройств, входящих в состав ОИ, а также выборочного контроля за выполнением требований НПА).

В результате были определены следующие исходные данные для обнаружения нерегламентируемой деятельности пользователей:

количество ОИ;

условия размещения ОИ;

состав ОИ;

время, прошедшее после предыдущего контроля;

форма проверки;

глубина проверки;

время, отводимое на проведение проверки;

наличие специализированных компьютерных программ для обнаружения нерегламентируемой деятельности пользователей.

Так как обнаружение нерегламентируемой деятельности пользователей на автономных ОИ возможно только в ходе

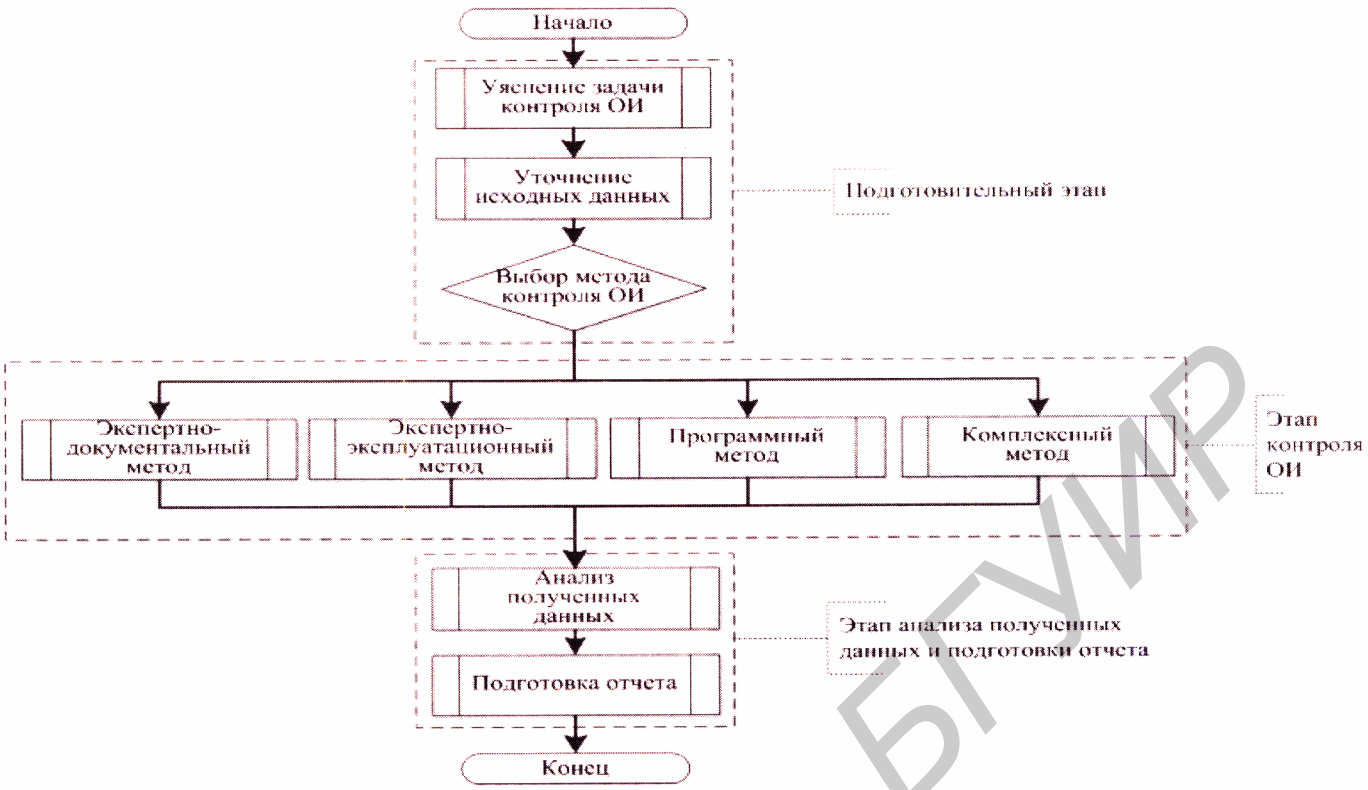

Рисунок 2. — Содержание и очередность этапов обнаружения нерегламентируемой деятельности пользователей на ОИ

контроля (наблюдения) деятельности самих пользователей и анализа полученных в ходе контроля данных, формирование методики свелось к описанию ряда последовательно выполняемых этапов (рисунок 2):

подготовительный этап;

этап контроля ОИ;

этап анализа полученных данных и подготовки отчета.

Указанная схема обеспечивает наглядность и простоту восприятия специалистом порядка осуществления обнаружения нерегламентируемой деятельности пользователей ОИ. Четкое выполнение им действий, отраженных в содержании этапов, позволяет проводить проверку ОИ с требуемым качеством. Полученный в результате необходимой корректировки схемы алгоритм можно применять для автоматизации процессов контроля действий пользователей ОИ (разработки специального программного обеспечения).

Подготовительный этап подразумевает выбор специалистом только одного из всего перечня предложенных методов контроля ОИ. Критериями для выбора являются указанные выше исходные данные, в том числе:

форма проверки с учетом полученной задачи и заданной глубины;

количество подлежащих проверке ОИ;

условия размещения и состав ОИ;

расчетное минимальное среднее значение времени, необходимое для проверки каждого ОИ;

отведенное на проведение проверки время;

наличие специализированных компьютерных программ;

общее количество привлекаемых к проведению проверки ОИ специалистов.

Этап контроля в алгоритме наиболее важный. Непосредственно в ходе него осуществляется контроль деятельности пользователей ОИ выбранным экспертно-документальным (экспертно-эксплуатационным, программным или комплексным) методом.

Сравнительная характеристика указанных методов сведена в таблицу 1.

Следует отметить, что, на первый взгляд, экспертно-документальный метод может быть наиболее востребованным методом контроля в ВС, так как не требует наличия

Таблица 1. — Сравнительная характеристика методов контроля ОИ

Метод контроля ОИ	Наличие специализированных компьютерных программ	Для каких форм контроля используется	Достигаемая глубина проверки	Время, необходимое для проведения контроля
Экспертно-документальный	Не требуется	Постоянный и повторный контроль	Поверхностная проверка	Минимальное
Экспертно-эксплуатационный		Внезапный, периодический и повторный контроль	Быстрая проверка	Максимальное
Программный	Требуется			Минимальное
Комплексный		Постоянный и повторный контроль	Тщательная проверка	Максимальное

особых знаний (навыков) у специалиста и использования им каких-либо специализированных компьютерных программ, выполнения в связи с этим дополнительных действий (рисунок 3).

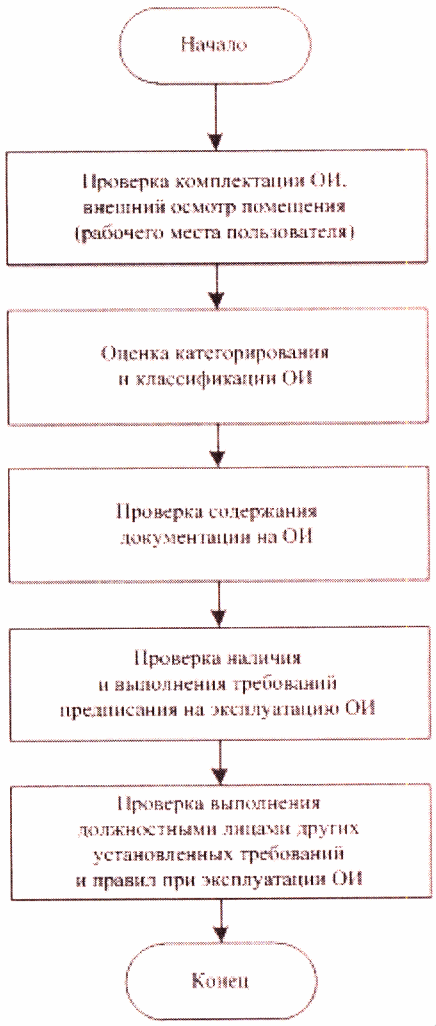

Рисунок 3. — Схема последовательности действий специалиста при экспертно-документальном методе контроля ОИ

Однако очевидно, что более высокое качество контроля и, соответственно, приемлемая глубина проверки будут достигаться в случае применения специалистом других методов: экспертно-эксплуатационного, программного и комплексного. В них дополнительно предусмотрены просмотр настроек установленной на ОИ операционной системы (содержимого МНИ и файлов, перечня распечатанных документов и т. д.), а также использование специализированных компьютерных программ для снижения влияния человеческого фактора на получаемые данные, уменьшения времени и расширения границ контроля ОИ.

На завершающем этапе анализа выполняются обработка полученных в ходе контроля данных и принятие решения о наличии фактов нерегламентируемой деятельности пользователей ОИ, а также определение мер противодействия их деятельности.

Для создания оснований наступления правовых последствий (привлечения виновных лиц к ответственности), организации учета инцидентов и накопления практического опыта осуществляется подготовка отчета. С учетом возможного дальнейшего использования результатов проверок отчет должен содержать полную информацию:

об условиях проведения проверки;

о характеристиках объектов проверки (ОИ и всех связанных с ним сведений);

о фактах нерегламентируемой деятельности, вскрытых в ходе проверки, и их характерных признаках;

о потенциальных последствиях фактов нерегламентируемой деятельности;

о вопросах, требующих решения начальника, назначившего проверку, или необходимости проведения дополнительной проверки.

В ситуациях, когда имеют место факты нерегламентируемой деятельности, по результатам проведенного специалистом анализа целесообразно:

сформировать «портрет» проверенного пользователя ОИ (рисунок 4), нарушившего установленные требования, посредством построения диаграммы из конкретных значений свойственных ему характеристик;

определить вероятные (вскрытые) цели атаки пользователя ОИ;

оценить потенциальный ущерб от действий пользователя ОИ.

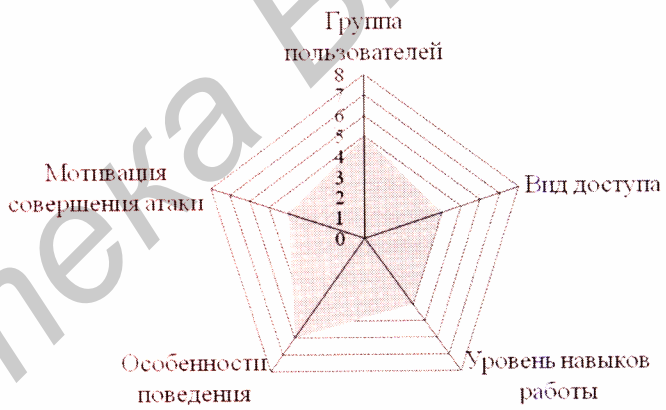

Рисунок 4. — Схема варианта «портрета» пользователя ОИ

Высокие значения характеристик пользователя ОИ («портрет», занимающий большую площадь диаграммы) в совокупности с наибольшим количеством целей для атаки будут указывать на более существенный потенциальный ущерб информационным ресурсам и инфраструктуре ИС от его действий. Развитием вышеуказанного этапа может быть разработка и внедрение в практику применения математической модели, позволяющей рассчитывать площадь «портрета» пользователя и вероятность нанесения ущерба информационным ресурсам. При этом оператор получит возможность обоснованно и своевременно ограничивать (блокировать) их доступ к ОИ в случае превышения определенных пороговых значений.

Таким образом, разработанная методика обнаружения нерегламентированной деятельности пользователей в полной мере раскрывает процесс выявления фактов нарушения пользователями установленных правил, вмешательства их в процесс эксплуатации ОИ и (или) использования МНИ и информационных ресурсов в различных целях, а также предоставления таких возможностей другим лицам. Ее наличие и необходимость применения обусловлена тем, что

на текущем этапе в ВС эксплуатируется большое количество автономных ОИ. Вместе с тем соответствующим органам и исполнителям необходимо осуществлять контроль соблюдения пользователями таких ОИ требований по защите информации. Методика имеет потенциал совершенствования, так как авторами видится возможным доработка и применение ее для проверок порядка использования сетей терминальной архитектуры и информационных сетей органов военного управления, объединенных корпоративной информационной сетью ВС.

ЛИТЕРАТУРА

1. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь от 10 нояб. 2008 г., № 455-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2016.

2. Защита информации. Основные термины и определения: СТБ ГОСТ Р 50922–2000. — Введ. 22.05.2000. — Минск: Гос. проектное и науч.-исслед. предприятие «Гипросвязь», 2000.

3. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация: СТБ 34.101.30–2007. — Введ. 28.09.2007. — Минск: Гос. науч. учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси», 2007.

4. Разработка методики обнаружения нерегламентируемой деятельности пользователей на объектах информатизации «средство вычислительной техники» (шифр «Брешь»): отчет о НИР (заключит.) / Науч.-исслед. ин-т Вооруженных Сил Респ. Беларусь; рук. Л.Л. Утин. — Минск, 2015. — 149 с.

Статья поступила в редколлегию 21.03.2016.