УДК 004.56

СУБЪЕКТНО-ОБЪЕКТНЫЕ ОТНОШЕНИЯ В УСЛОВИЯХ РАЗНОРОДНЫХ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕГРИРОВАННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

© 2015 С. В. Скрыль, Д. Г. Зыбин

Воронежский институт ФСИН России, ул. Иркутская, 1а, 394072, г. Воронеж, Россия
E-mail: zdg77@mail.ru

Поступила в редакцию 21.02.2015 г.

Аннотация. Рассматриваются компоненты субъектно-объектных отношений, характерных для информационных процессов в интегрированных системах безопасности (ИСБ) и процессах защиты информации в условиях их функциональной независимости и зависимости. Обосновываются определения функционально независимой и функционально зависимой систем защиты информации в ИСБ.

Ключевые слова: интегрированные системы безопасности, функционально независимая система защиты информации, функционально зависимая система защиты информации.

В основе концепции обеспечения защиты информации в ИСБ лежит разделение субъекта и объекта деятельности [1]. Субъектно-объектные отношения в процессе информационной деятельности проявляются через определенные потребности, возникающие, когда в результате восприятия, анализа и сравнения информации об объекте субъект может прийти к выводу о том, что его состояние и тенденции развития являются неудовлетворительными и требуют приведения в желательное состояние. Удовлетворенная потребность составляет целевую функцию информационной деятельности [2].

Для удовлетворения потребности субъект должен осуществить комплекс действий, направленных на перевод объекта в желательное состояние. Таким образом, необходимым признаком субъектно-объектных отношений является активность субъекта, реализующая целевую функцию информационной деятельности.

Особенностью охранной деятельности на современном этапе ее развития является то, что достижение ее нормативно определенных целей связано с использованием ИСБ – систем с высоким уровнем информатизации, в связи с чем и сами информационные процессы в ИСБ являются строго регламентированными соответствующими нормативами.

При этом информационные процессы в ИСБ представляются как процессы с функциональным разделением, где под субъектами информационной деятельности понимаются элементы структуры ИСБ.

Целенаправленная деятельность по защите информации в ИСБ может быть представлена в виде последовательности процедур анализа признаков воздействия угроз информационной безопасности на информационные процессы в ИСБ.

Предпосылкой такой деятельности является то, что информационные процессы в ИСБ реализуются в условиях постоянно действующих угроз безопасности со стороны агрессивной среды (АС), под которой понимается организационная структура любого рода, целью информационной деятельности которой являются противоправные действия в отношении информации ИСБ для создания условий проникновения на охраняемый объект [3].

Основными задачами информационной деятельности АС как источника формирования угроз безопасности информации в ИСБ являются действия, направленные на ее несанкционированный съем, копирование, искажение и блокирование.

Это обусловило необходимость дополнения информационных процессов в ИСБ процессами обеспечения защиты информации, реализуемых с целью:

– выявления и локализации источников угроз безопасности информации;

– принятия мер по подавлению указанных источников;

– восстановления корректности информационных процессов в ИСБ.

В информационном плане это позволяет представить ИСБ как систему, состоящую из двух функциональных подсистем: подсистемы сбора, обработки информации и управления и подсистемы защиты информации. Вместе с тем, трактуя понятие «система», в независимости от учитываемых факторов и степени абстрактности [1; 2; 4], как совокупность элементов со способностью каждого выполнять собственные предметные функции в соответствии с заданными критериями, эти подсистемы можно рассматривать как самостоятельные системы – систему сбора, обработки информации и управления (ССОИУ) и систему защиты информации (СЗИ).

Обеспечение защиты информации в ИСБ имеет определенные особенности, обусловленные, прежде всего, тем, что субъектно-объектные отношения в этих условиях реализуются тремя видами информационных процессов. При этом все субъекты для достижения собственных целей воздействуют на один и тот же объект.

Субъектами информационной деятельности в данном контексте являются:

– ССОИУ, активность которой направлена на решение задач, связанных с охраной объекта;

– АС, осуществляющая свою активность с целью несанкционированного съема, копирования, искажения и блокирования информации ИСБ;

– СЗИ, активность которой направлена на противодействие цели агрессивной среды.

В отношении реализации СЗИ возможны два концептуальных подхода.

Первый подход предполагает независимость функций обработки информации в ССОИУ и функций ее защиты. В этом случае субъектно-объектные отношения, характерные для информационных процессов ИСБ в рассматриваемых условиях, определяются следующими компонентами (рис. 1):

– информационная потребность 1 ИСБ – информационное обеспечение решения задач, связанных с охраной объекта;

– цель 1 информационного процесса в ИСБ – реализация информационной потребности 1;

– субъект информационной деятельности – ССОИУ;

– практическая активность 1 ССОИУ, как субъекта информационной деятельности осуществляемая для достижения цели 1;

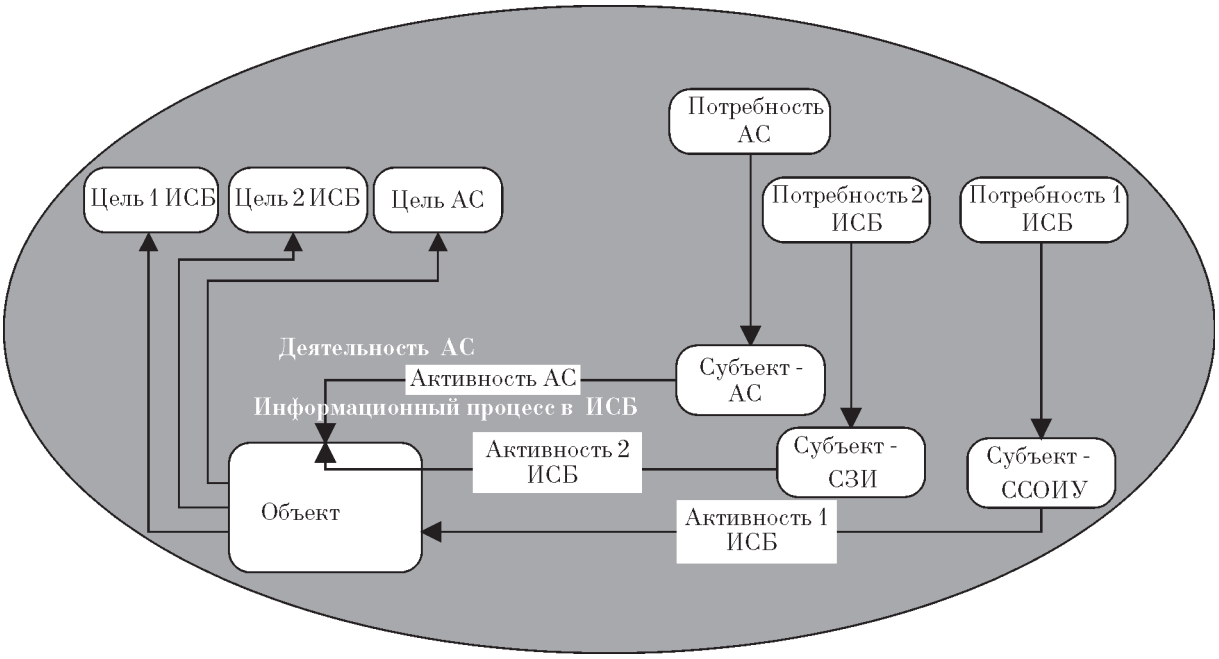

Рис. 1. Субъектно-объектные отношения в условиях независимости информационных процессов в ИСБ и процессов защиты информации

– информационная потребность 2 ИСБ – решение задач защиты информации;

– цель 2 реализации информационного процесса в ИСБ – обеспечение информационной потребности 2;

– субъект информационной деятельности по защите информации в ИСБ – СЗИ;

– практическая активность 2 СЗИ как субъекта информационной деятельности, осуществляемая для достижения цели 2;

– информационная потребность ИСБ – информационное обеспечение решения задач, связанных с охраной объекта;

– цель информационной деятельности АС – реализация ее информационной потребности;

– субъект информационной деятельности – АС;

– практическая активность АС как субъекта информационной деятельности, осуществляемая для достижения ее цели;

– объект – состояние физической защищенности охраняемого объекта.

Второй подход предполагает зависимость информационных процессов в ИСБ и процессов защиты информации. Следствием этого является реализация этих потребностей одним субъектом информационной деятельности – ССОИУ ИСБ с внедренными в ее информационные процессы функциями СЗИ. В этих условиях субъект проявляет единую практическую активность по достижению целей, обусловленных такими потребностями. В этом случае субъектно-объектные отношения, характерные для информационных процессов ИСБ в рассматриваемых условиях, определяются следующими компонентами (рис. 2):

– информационная потребность 1 ИСБ – информационное обеспечение решения задач, связанных с охраной объекта;

– информационная потребность 2 ИСБ – решение задач защиты информации в условиях угроз ее безопасности;

– цель 1 реализации информационных процессов в ИСБ – обеспечение информационной потребности 1;

– цель 2 реализации информационных процессов в ИСБ – обеспечение информационной потребности 2;

– субъект информационной деятельности – ССОИУ с внедренными в ее информационные процессы функциями СЗИ;

– практическая активность 1 ИСБ как субъекта информационной деятельности направлена на достижение целей 1 и 2;

– информационная потребность АС – решение задач ее информационной деятельности;

– цель информационной деятельности АС – реализация ее информационной потребности;

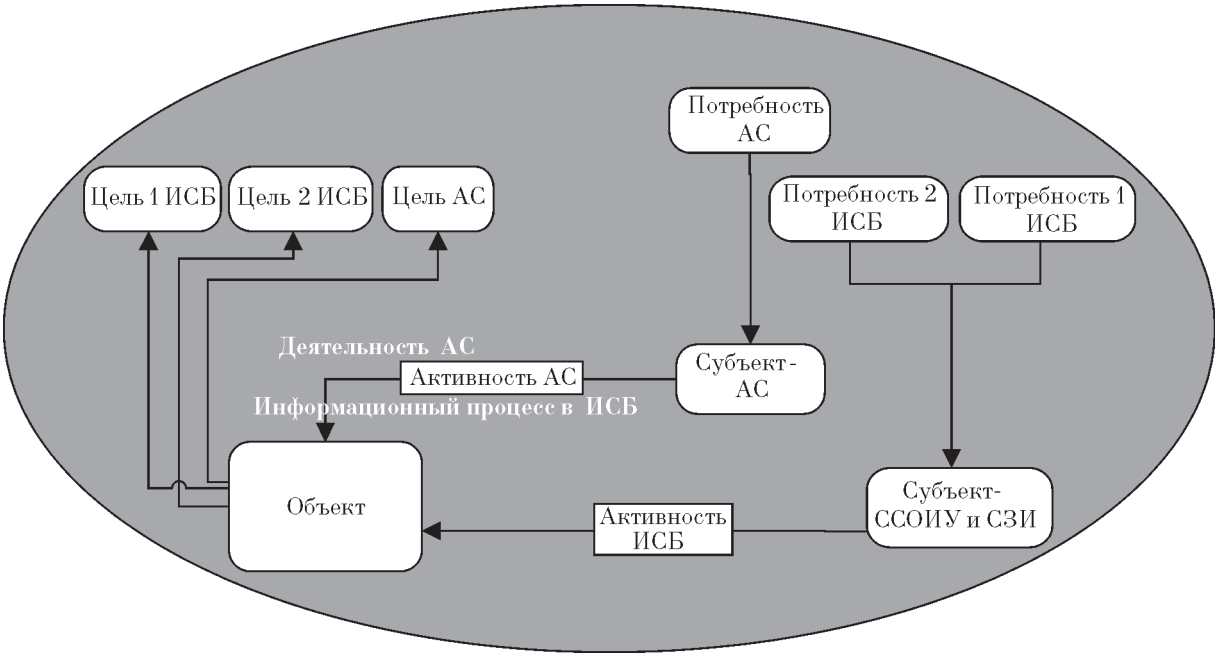

Рис. 2. Субъектно-объектные отношения в условиях зависимости информационных процессов в ИСБ и процессов защиты информации

– субъект информационной деятельности – АС;

– практическая активность АС как субъекта информационной деятельности, осуществляемая для достижения ее цели;

– объект – состояние физической защищенности охраняемого объекта.

Как следует из изложенного, второй подход к реализации СЗИ ИСБ предполагает отсутствие отдельного субъекта, а следовательно, и отдельной функциональной структуры для обеспечения информационной потребности данного вида.

С целью определения условий независимости и зависимости информационных процессов в ИСБ и процессов защиты информации рассмотрим понятие функциональной структуры системы.

Известно достаточно много определений понятия «структура» [1; 2; 4]. Мы будем понимать под структурой некоторую семантическую конструкцию, описывающую языковыми средствами – естественным языком, средствами математики и другими – определенную совокупность элементов и связи между ними.

В соответствии с введенным определением и общепринятым пониманием функциональная структура как ССОИУ ИСБ, так и ее СЗИ представляет собой состав выполняемых функций характеризующихся:

– их количеством;

– качеством каждой функции с точки зрения ее способности и возможности выполнения;

– взаимосвязями между функциями в процессе функционирования ССОИУ и СЗИ;

– ориентированностью отдельных групп функций;

– реализуемостью на отдельных пространственно распределенных элементах ССОИУ и СЗИ.

Это дает возможность представлять СЗИ в ИСБ в двух вариантах: как структуру, выполняющую свои задачи собственной совокупностью функций, либо как структуру, выполняющую свои задачи на совокупности функций ССОИУ.

В первом случае СЗИ является функционально независимой от ССОИУ, во втором – функционально зависимой. Сформулируем определения такого рода системы.

Функционально независимой СЗИ в ИСБ будем называть систему, которая реализует процесс защиты информации за счет использования собственных механизмов, ресурсов и исполнителей, а функционально зависимой – систему, которая в качестве собственных элементов использует механизмы и ресурсы ССОИУ, а также ее персонал.

Следует отметить, что функциональная сложность СЗИ естественным образом приводит к значительному усложнению ее описания. Следствием подобного усложнения является наличие двух уровней описания СЗИ: функционального и технического.

На функциональном уровне СЗИ описывается упорядоченной, в соответствии с логикой информационных процессов в ССОИУ ИСБ, совокупностью взаимосвязанных процедур защиты информации.

На техническом уровне СЗИ описывается совокупностью операций, выполняемых программными и программно-аппаратными средствами при реализации соответствующих алгоритмов обнаружения угроз безопасности информации, принятия решения по подавлению их источников и устранению последствий возникновения.

Рассмотренные основания позволяют сформировать методические основы комплексного использования разнородных подходов к обеспечению защиты информации в ИСБ.

СПИСОК ЛИТЕРАТУРЫ

1. *Скрыль С. В.* Основы системного анализа в защите информации : учеб. пособие для студентов высших учебных заведений / С. В. Скрыль, А. А. Шелупанов. – М. : Машиностроение, 2008. – 138 с.

2. Информатика : учебник для высших учебных заведений МВД России : в 2 т. Т. 1. Концептуальные основы / В. А. Минаев, С. В. Скрыль, С. В. Дворянкин, Н. С. Хохлов [и др.]. – М. : Маросейка, 2008. – 464 с.

3. *Зарубин В. С.* Классификация информационных угроз интегрированных систем безопасности / В. С. Зарубин, С. В. Гурченко, А. Р. Фамильнов // Информация и безопасность : региональный научно-технический журнал. – 2009. – Т. 12, ч. 3. – С. 425–428.

4. Основы информационной безопасности : учебник для высших учебных заведений МВД России / под ред. С. В. Скрыля, В. А. Минаева. – Воронеж : Воронежский институт МВД России, 2001. – 464 с.

THE SUBJECT AND OBJECT RELATIONS IN THE CONDITIONS OF DIVERSE APPROACHES TO ENSURING INFORMATION SECURITY IN THE INTEGRATED SECURITY SYSTEMS

© 2015 S. V. Skryl, D. G. Zybin

Voronezh institute of the Russian Federal Penitentiary Service,
Irkutskaya St., 1a, 394072, Voronezh, Russia
E-mail: zdg77@mail.ru

Received 21.02.2015

Annotation. Components of the subject and object relations, characteristic to information processes in the integrated security systems and to processes of information security in the conditions of their functional independence and dependence are considered. Definitions of functional and independent and functional and dependent systems of information security locate in the integrated security systems.
Keywords: the integrated security systems, functional and independent system of information security, functional and dependent system of information security.

REFERENCES

1. Skryl' S. V., Shelupanov A. A. *Osnovy sistemnogo analiza v zashchite informatsii*, Moscow, Mashinostroenie, 2008, 138 p.

2. Minaev V. A., Skryl' S. V., Dvoryankin S. V., Khokhlov N. S. *Informatika : uchebnik dlya vysshikh uchebnykh zavedenii MVD Rossii Kn. 1.: Kontseptual'nye osnovy*, Moscow, Maroseika, 2008, 464 p.

3. Zarubin V. S., Gurchenko S. V., Famil'nov A. R. Klassifikatsiya informatsionnykh ugroz integrirovannykh sistem bezopasnosti. *Informatsiya i bezopasnost': regional'nyi nauchno-tekhnicheskii zhurnal*, 2009, vol. 12, pt. 3, pp. 425–428.

4. Skryl' S. V., Minaev V. A. *Osnovy informatsionnoi bezopasnosti : uchebnik dlya vysshikh uchebnykh zavedenii MVD Rossii*, Voronezh, Voronezhskii institut MVD Rossii, 2001, 464 p.

Скрыль Сергей Васильевич – профессор кафедры технических комплексов охраны и связи Воронежского института ФСИН России, доктор технических наук, профессор.

Зыбин Дмитрий Георгиевич – заместитель начальника Воронежского института ФСИН России по научной работе, кандидат технических наук, доцент. E-mail: zdg77@mail.ru

Skryl Sergey Vasilyevich – professor of Voronezh institute of the Russian Federal Penitentiary Service, the doctor of technical sciences, professor.

Zybin Dmitri Georgievich – deputy director of the institute for science of Voronezh institute of the Russian Federal Penitentiary Service, the candidate of technical sciences, associate professor. E-mail: zdg77@mail.ru