УДК 002.001;002:001.8

В.Н. Финько, В.В. Киселев, В.К. Джоган, В.В. Шерстобитов, Е.Б. Белов, А.А. Шелупанов

Концептуальные понятия деятельности по защите информации

Рассматриваются концептуальные понятия защиты информации с позиций представления о ее вспомогательным виде деятельности. Обосновывается набор базовых процедур защиты информации.

Любого рода информационная деятельность невозможна без осуществления вспомогательных (обеспечивающих) видов деятельности, непосредственно не преследующих нормативно определенных целей, но необходимых для их достижения. Одним из таких видов деятельности является защита информации. Этим термином обозначается регулярная деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [1]. Рассмотрим содержание и дадим определения основных компонентов этого понятия.

Необходимость защиты информации существует в случае ее конфиденциальности, под которой понимается свойство, позволяющее не давать право на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам [1].

Из этого следует, что потребность в защите информации - это определенное состояние субъекта информационной деятельности, которое возникает в связи с необходимостью защиты сведений, обеспечивающих решение его задач. При этом проблема выявления, описания и измерения потребностей в обеспечении конфиденциальности информации становится одной из основных в комплексе проблем защиты информации. Только на основе ее решения можно формулировать требования к защищенности информационной деятельности.

Потребности в защите информации определяют ее цель, которая состоит в обеспечении защищенности информационной деятельности. При этом под защищенностью информации понимается соответствие эффективности защиты информации требованиям нормативных документов [1].

В качестве субъекта защиты информации могут выступать:

- специализированные подразделения, обеспечивающие:

– оборот документов, содержащих сведения, составляющие государственную и служебную тайну, их хранение и уничтожение, а также контроль над правильностью оборота таких документов;

– криптографическую защиту информации, передаваемой по каналам связи, а также учет и хранение документов, переданных по каналам связи;

– проведение комплекса мероприятий, направленных на исключение возможности утечки сведений, составляющих государственную и служебную тайну, по так называемым «побочным» каналам (сети электропитания, радиотрансляция и т.п.);

- сотрудники, реализующие свою информационную деятельность в условиях обеспечения ее конфиденциальности.

Структурирование основных компонентов является необходимым, но недостаточным условием понимания сущности деятельности, так как не учитывает ряда факторов, непосредственно не входящих в понятие, но создающих определенную обстановку (среду), в которой осуществляется деятельность.

Среду деятельности по защите информации составляют сфера доминирования и неуправляемая сфера. К сфере доминирования относят средства, которыми располагает субъект деятельности, и элементы окружающей действительности, на которые он может воздействовать. Неуправляемую сферу образует группа элементов, на которые субъект деятельности не может воздействовать, но которые необходимо учитывать в виде ограничений.

В рамках среды определяется необходимый и достаточный набор активностей (процедур) по достижению целей защиты информации.

Будем называть процедурой защиты информации набор однородных в функциональном отношении действий (операций), регулярно осуществляемых субъектами по обеспечению защищенности своей информационной деятельности. Целями реализации процедур защиты информации являются закрытие информации или ее криптопреобразование инвариантно способу реализации процедуры и используемым средствам. Информация здесь рассматривается нами как предмет защиты (используемый специфический ресурс).

Совокупность логически упорядоченных, взаимосвязанных и организованных процедур защиты информации, ведущая к достижению цели обеспечения защищенности информационной деятельности, составляет процесс защиты информации.

В общем случае процесс защиты информации может включать следующие процедуры: идентификация и аутентификация, паролирование и управление доступом к информации, учет событий, контроль состояния защиты информации, шифрование. Содержание перечисленных процедур приведено в таблице.

Наименование процедуры	Содержание процедуры	Используемая терминология
Идентификация	Сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [2]	Идентификатор доступа – уникальный признак субъекта или объекта доступа [2]. Объект доступа – единица информационного ресурса защищенной информационной системы, доступ к которой регламентируется правилами разграничения доступа [2]. Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа [2]
Аутентификация	Подтверждение подлинности [3]	
Паролирование доступа	Использование пароля	Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом [2]
Управление доступом	Предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение использования ресурса неполномочным способом [3]	Ресурсы (подлежащие защите): – информация и данные (включая программное обеспечение и относящиеся к средствам защиты пассивные данные, такие как пароли); – услуги передачи и обработки данных; – оборудование и средства [3]
Учет событий	Регистрация собственных действий любого логического объекта	
Контроль состояния защиты информации	Проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам защиты информации [4]	
Шифрование	Криптографическое преобразование данных для получения шифротекста [3]	Шифротекст – данные, получаемые в результате использования шифрования [3]

Очевидно, что формирование компетенций специалистов должно основываться на понятийном аппарате в области защиты информации и информационной безопасности [5, 6]. Понятийный базис обеспечивает единство признаваемых требований. Таким образом можно формировать компетенции специалистов на базе концептуальных понятий деятельности в области защиты информации.

Это особенно важно при подготовке специалистов в области защиты информации и информационной безопасности. Опыт проведения курсов «Основы информационной безопасности» и «Комплексное обеспечение информационной безопасности автоматизированных систем» на кафедре Комплексной информационной безопасности электронно-вычислительных систем Томского государственного университета систем управления и радиоэлектроники показали необходимость формирования единого понятийного базиса.

Кроме того, анализ квалификации сотрудников отделов защиты информации Пенсионного фонда России (повышение квалификации которых проводилось на базе Центра технологий безопасности ТУСУРа) показал, что подготовка понятийного аппарата, соответствующего всем нормам [1-4] требует не только аккуратного обращения с терминами и определениями, но и четкого выстраивания логически упорядоченных взаимосвязей.

Литература

1. Информационная безопасность и защита информации: Сб. терминов и определений. – М.: Гостехкомиссия России, 2001. – 149 с.

2. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ // Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: Гостехкомиссия России, 1998.

3. ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 1. Архитектура защиты информации.

4. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

5. ГОСТ ИСО МЭК 15408–2002 Критерии оценки безопасности информационных технологий.

5. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.

Финько Владимир Николаевич

Киселев Вадим.Вячеславович

Джоган Василий Климович

Шерстобитов Владислав Викторович

Белов Евгений Борисович
ИКСИИ, 93 106 09

Шелупанов Александр Александрович
ГОУ ВПО Томский государственный университет систем управления и радиоэлектроники
Зав. кафедрой Комплексной информационной безопасности электронно-вычислительных систем, д.т.н., профессор
Эл. адрес: saa@keva.tusur.ru

V.N. Finko, V.V. Kiselev, V.K. Djzogan, V.V. Sherstobitov, E.B. Belov, A.A. Shelupanov
Activity concepts on information protection

Are considered concepts of information protection the from positions of representation by its auxiliary kind of an information process. The set of base protection procedures of the information proves.