Лекция 4. Пути реализации функций управления механизмами обеспечения защиты информации.

1. Возможные пути реализации функции в управлении механизмами обеспечения защиты информации.

Защита информации — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Система называется безопасной, если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Очевидно, что абсолютно безопасных систем нет, и здесь речь идет о надежной системе в смысле «система, которой можно доверять» (как можно доверять человеку). Система считается надежной, если она с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются: *политика безопасности и гарантированность*.

Политика безопасности, являясь активным компонентом защиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации. Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.

Гарантированность, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности (должен использоваться механизм подотчетности протоколирования, дополняющийся анализом запомненной информации, то есть аудитом).

При оценке степени гарантированности, с которой систему можно считать надежной, центральное место занимает достоверная (надежная) вычислительная база. Достоверная вычислительная база (ДВБ) представляет собой полную совокупность защитных механизмов компьютерной системы, которая используется для претворения в жизнь соответствующей политики безопасности.

Функции непосредственной защиты информации.

1. Предупреждение возникновения условий, благоприятствующих порождению (возникновению) дестабилизирующих факторов. Главной целью данной функции является способствование такому построению архитектуры информационной системы (ИС), технологических схем автоматизированной обработки информации и их обеспечению, чтобы свести к минимуму саму возможность появления дестабилизирующих факторов во всех потенциально возможных условиях функционирования ИС. Иными словами — преследуется упреждающая цель.

2. Предупреждение непосредственного проявления дестабилизирующих факторов в конкретных условиях функционирования ИС. Выделением данной функции также преследуется цель упреждения возникновения дестабилизирующих факторов, однако в отличие от предыдущей функции, осуществляемой с целью общего предупреждения, мероприятия функции 2 предполагается осуществлять для предупреждения

проявления дестабилизирующих факторов в конкретных условиях жизнедеятельности ИС.

3. Обнаружение проявившихся дестабилизирующих факторов. Предполагается осуществление таких мероприятий, в результате которых проявившиеся дестабилизирующие факторы (или реальная угроза их проявления) будут обнаружены еще до того, как они окажут воздействие на защищаемую информацию. Иными словами, это функция непрерывного слежения за дестабилизирующими факторами.

4. Предупреждение воздействия дестабилизирующих факторов на защищаемую информацию. Само название функции говорит о ее содержании: мероприятия, осуществляемые в рамках данной функции, преследуют цель не допустить нежелательного воздействия дестабилизирующих факторов на защищаемую информацию даже в том случае, если они реально проявились, т. е. данная функция является естественным продолжением предыдущей. Однако осуществление предыдущей функции может быть как успешным (проявление дестабилизирующих факторов будет обнаружено), так и неуспешным (проявление дестабилизирующих факторов не будет обнаружено). С целью же создания условий для надежной защиты информации в рамках данной функции, вообще говоря, должны быть предусмотрены мероприятия по предупреждению воздействия дестабилизирующих факторов на информацию в любых условиях. С учетом этого обстоятельства функцию предупреждения воздействия целесообразно разделить на две составные: предупреждение воздействия на информацию проявившихся и обнаруженных дестабилизирующих факторов и предупреждение воздействия на информацию проявившихся, но не обнаруженных дестабилизирующих; факторов.

5. Обнаружение воздействия дестабилизирующих факторов на, защищаемую информацию. Нетрудно видеть, что основное содержание мероприятий данной функции аналогично содержанию мероприятий функции 3 с той разницей, что если функция 3 есть функция слежения за

дестабилизирующими факторами, то рассматриваемая функция есть функция слежения за компонентами защищаемой информации с целью своевременного обнаружения фактов воздействия на них дестабилизирующих факторов. При этом под своевременным понимается такое обнаружение, при котором сохраняются реальные возможности локализации воздействия на информацию, т. е. предупреждения распространения его в нежелательных размерах.

6. Локализация воздействия дестабилизирующих факторов на информацию. Являясь логическим продолжением предыдущей, данная функция предусмотрена с целью недопущения распространения воздействия на информацию за пределы максимально допустимых размеров. Но в рамках данной функции должны быть предусмотрены мероприятия как на случай успешного осуществления функции 5 (воздействие дестабилизирующих факторов на информацию обнаружено), так и на случай неуспешного ее осуществления (указанное воздействие не обнаружено). Тогда аналогично функции 4 рассматриваемую функцию также целесообразно разделить на две составные: локализацию обнаруженного воздействия дестабилизирующих факторов на информацию и локализацию необнаруженного воздействия.

7. Ликвидация последствий воздействия дестабилизирующих факторов на защищаемую информацию. Под ликвидацией последствий понимается проведение таких мероприятии относительно локализованного воздействия дестабилизирующих факторов на информацию, в результате которых дальнейшая обработка информации может осуществляться без учета имевшего место воздействия. Иными словами, удается восстановить то состояние защищаемой информации, которое имело место до воздействия дестабилизирующих факторов. Совершенно очевидно, что механизмы, с помощью которых могут быть .ликвидированы последствия воздействия, в общем случае будут различными для случаев локализации обнаруженного и необнаруженного воздействия. Тогда аналогично предыдущему эту функцию целесообразно представить в виде двух составных: ликвидация последствий

обнаруженного и локализованного воздействия дестабилизирующих факторов на защищаемую информацию и ликвидация последствий локализованного, но не обнаруженного воздействия на информацию.

2. Сведение репрезентативного множества задач защиты в классы.

Осуществление функций защиты в ИС достигается решением задач защиты, причем под задачей защиты понимаются организованные возможности средств, методов и мероприятий, реализуемых в ИС с целью полного или частичного осуществления одной или нескольких функций защиты в одной или нескольких зонах защиты.

В механизмах защиты информации, очевидно, должны быть предусмотрены задачи для осуществления всех функций защиты во всех зонах защиты, относительно обоих видов защиты и всех дестабилизирующих факторов. Обозначим: *Ф* - множество функций защиты; *З* - множество зон защиты; *В* - множество видов защиты; *Д* - множество дестабилизирующих факторов, влияющих на защищенность информации. Тогда множество задач защиты *З** определяется как декартово произведение перечисленных выше множеств, т.е.

З = ФхЗхВхД.*

Из предыдущего следуют оценки множеств, определяющих размерность множества задач защиты: *Ф* - общее число функций защиты первого вида = 10; *З* - общее число зон защиты = 5; *В* - общее число видов защиты = 2 (рассматриваем только обеспечение целостности информации к предупреждение несанкционированного ее получения); *Д* - общее числе дестабилизирующих факторов: 133 ПНЦИ и 67 КНПИ.

Тогда: *З* = 10х5х (133 + 67) = 10 х5 х200 = 10000*

Таким образом, множество задач защиты для самого общего случая должно включать 10000 групп задач. Размерность этого множества можно существенно уменьшить за счет унификации, т.е. формирования таких задач,

каждая из которых могла бы входить в несколько групп. Для этого, необходимо прежде всего произвести системную классификацию задач. Основой для классификации может стать предметный анализ объективных возможностей осуществления функций защиты. Результаты анализа приведены в табл. 16.1 (для функций обеспечения защиты).

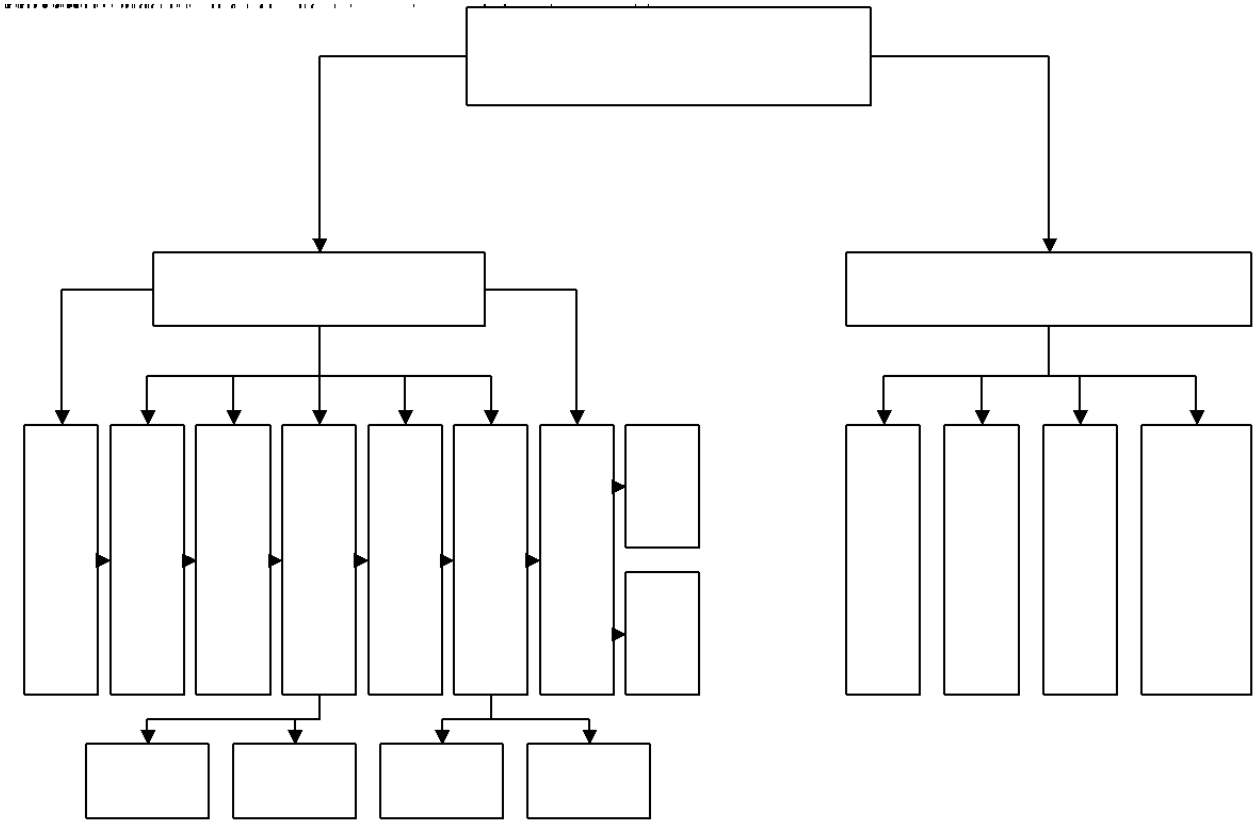

Таблица 16.1

№ функции	Функция	Пути реализации на этапах жизненного цикла ИС		
		Создание	Внедрение	Эксплуатация
1	Предупреждение проявления условий, благоприятных для порождения дестабилизирующих факторов	1.Обоснование требований к защите информации по всей совокупности показателей 2.Формирование множества ожидаемых дестабилизирующих факторов 3.Оценка возможных значений характеристик дестабилизирующих факторов 4.Проектирование компонентов системы, устойчивых к дестабилизирующим факторам	1.Проверка и уточнение требований к защите информации 2.Проверка и уточнение дестабилизирующих факторов 3.Проверка проектных решений на устойчивость к дестабилизирующим факторам 4.Корректировка проектных решений	1.Обеспечение работы механизмов предупреждения 2.Контроль работы механизмов предупреждения 3.Сбор и обработка статических данных о работе механизмов предупреждения 4.Разработка предложений по совершенствованию механизмов предупреждения
2	Предупреждение проявления дестабилизирующих факторов	1.Обоснование требований к механизмам слежения за функционированием компонентов предупреждения появления условий, предусмотренных функцией №1 2.Проектирвание механизмов слежения 3.Проектирование механизмов воздействия на факторы, определяющие возможность появления условий, благоприятных для дестабилизирующих факторов	1.Проверка и уточнение требований к механизмам слежения 2.Проверка проектных решений по вопросам слежения 3.Корректировка проектных решений	1.Обеспечение работы механизмов слежения 2.Контроль работы механизмов слежения 3.Сбор и обработка данных о функционировании механизмов слежения 4.Разработка предложений по совершенствованию механизмов слежения

3	Обнаружение проявившихся дестабилизирующих факторов	1.Обоснование требований к механизмам контроля проявления ДФ 2.Изучение возможностей контроля ДФ 3.Обоснование структуры и состава механизмов контроля ДФ 4.Разработка средств контроля 5.Проектирование механизмов контроля	1.Проверка и уточнение требований к механизмам контроля проявления ДФ 2.Проверка эффективности механизмов контроля проявления ДФ 3.Корректировка проекта механизмов контроля	1.Обеспение работы механизмов контроля 2.Контроль работы механизмов контроля 3.Сбор и обработка статистических данных о работе механизмов контроля 4.Разработка предложений по совершенствованию механизмов контроля
4а	Нейтрализация дестабилизирующего воздействия обнаружения проявляющих факторов	1.Оценка ожидаемых потребностей в нейтрализации дестабилизирующего воздействия обнаруживаемых факторов 2.Обоснование требований к системе обработки, исходя из условий нейтрализации 3.Проектирование необходимых средств нейтрализации 4.Проектирование технологий нейтрализации воздействия обнаруживаемых факторов 5.Оценка ожидаемой эффективности нейтрализации дестабилизирующего воздействия обнаруживаемых факторов	1.Отладка средств и технологии нейтрализации дестабилизирующего воздействия обнаруживаемых факторов 2.Проверка эффективности механизмов нейтрализации 3.Корректировка проектных механизмов нейтрализации 4.Отработка технологии нейтрализации дестабилизирующего воздействия обнаруженных проявлений факторов	1.Слежение за проявлением дестабилизирующих факторов 2.Определение необходимости нейтрализации дестабилизирующего воздействия обнаруживаемых факторов 3.Выбор рациональных средств и методов нейтрализации 4.Реализация выбранных методов 5.Контроль нейтрализации 6.Сбор и обработка статистических данных об использовании средств и методов нейтрализации

				7.Разработка рекомендации по совершенствованию механизмов
4б	Нейтрализация дестабилизирующего воздействия необнаруженных проявившихся факторов	1.Оценка ожидаемых потребностей в нейтрализации дестабилизирующего воздействия необнаруженных проявившихся факторов 2.Обоснование требований к механизмам нейтрализации необнаруженных проявившихся факторов 3.Обоснование требований к системе обработки, исходя из условий нейтрализации необнаруженных проявившихся факторов 4.Разработка средств нейтрализации 5.Обоснование технологий нейтрализации дестабилизирующего воздействия необнаруженных проявившихся факторов 6.Оценка ожидаемой эффективности нейтрализации	1.Проверка эффективности механизмов нейтрализации дестабилизирующего воздействия необнаруженных проявившихся факторов 2.Корректировка проектных решений механизмов нейтрализации 3.Отладка технологий нейтрализации дестабилизирующего воздействия необнаруженных проявившихся факторов	1.Обеспечение работы механизмов нейтрализации 2.Сбор и обработка статистических данных о функционировании механизмов нейтрализации дестабилизирующего воздействия необнаруженных проявившихся факторов 3. Разработка рекомендации по совершенствованию соответствующих механизмов
5	Обнаружение снижения защиты информации	1.Обоснование требований к механизмам контроля защиты информации 2.Обоснование требований к системе обработки, исходя из условий контроля защиты информации	1.Проверка эффективности функционирования механизмов обнаружения снижения защиты информации 2.Корректировка проектных решений механизмов	1.Обеспечени функционирования 2.Контроль работы механизмов обнаружения

		3.Разработка средств и методов контроля защиты информации 4.Разработка технологии контроля защиты информации 5.Оценка эффективности механизмов обнаружения снижения защиты информации	обнаружения снижения защиты информации 3.Отладка технологии контроля защиты информации и обнаружения ее снижения	3.Сбор и обработка статистических данных о работе механизмов обнаружения 4.Разработка предложений по совершенствованию механизмов
6а	Локализация обнаружения снижения зашиты информации	1.Оценка ожидаемых потребностей в локализации обнаруживаемого снижения зашиты информации 2.Обоснование требований к системе обработки, исходя из условий локализации обнаруживаемого снижения зашиты информации 3.Проектирование необходимых средств локализации обнаруживаемого снижения зашиты информации 4.Проектирование технологий локализации обнаруживаемого снижения зашиты информации 5.Оценка ожидаемой эффективности локализации обнаруживаемого снижения зашиты информации	1.Отладка средств и технологии локализации обнаруживаемого снижения зашиты информации 2.Проверка эффективности механизмов локализации обнаруживаемого снижения зашиты информации 3.Корректировка проектных механизмов локализации обнаруживаемого снижения зашиты информации 4.Отработка технологии локализации обнаруживаемого снижения зашиты информации	1.Слежение за зашитой информации 2.Определение необходимости мест и размеров локализации обнаруживаемого снижения зашиты информации 3.Выбор рациональных средств и методов локализации 3.Реализация выбранных методов 5.Контроль локализации 6.Сбор и обработка статистических данных об использовании средств и методов локализации 7.Разработка рекомендации по совершенствованию механизмов

6б	Локализация необнаруженного снижения зашиты информации	1.Оценка ожидаемых потребностей необнаруженного снижения зашиты информации 2.Обоснование требований к механизмам локализации 3.Обоснование требований к системе обработки, исходя из условий локализации 4.Разработка средств локализации 5.Обоснование технологий локализации необнаруженного снижения зашиты информации 6.Оценка ожидаемой эффективности локализации	1.Проверка эффективности механизмов локализации 2.Корректировка проектных решений механизмов локализации	1.Обеспечение работы механизмов локализации 2.Сбор и обработка статистических данных о функционировании механизмов локализации 3. Разработка рекомендации по совершенствованию локализация необнаруженного снижения зашиты информации
7а	Восстановление обнаруженного нарушения зашиты информации	1.Оценка ожидаемых потребностей в восстановления информации 2.Обоснование требований к системе обработки, исходя из условий восстановления защиты информации 3.Проектирование необходимых средств восстановления защиты информации 4.Проектирование технологий восстановления информации 5.Оценка ожидаемой эффективности восстановления	1.Отладка средств и технологии восстановления информации 2.Проверка эффективности механизмов восстановления 3.Корректировка проектных механизмов восстановления 4.Отработка технологии восстановления защиты	1.Слежение за зашитой информации 2.Определение необходимости мест и размеров восстановления защиты информации 3.Выбор рациональных средств и методов восстановления 3.Реализация выбранных методов 5.Контроль восстановления

				6.Сбор и обработка статистических данных об функционировании механизмов восстановления
7б	Восстановление необнаруженного нарушения зашиты информации	1.Оценка ожидаемых потребностей в локализации необнаруженных нарушений зашиты информации 2.Обоснование требований к механизмам необнаруженных нарушений зашиты 3.Обоснование требований к системе обработки, исходя из условий необнаруженных нарушений зашиты 4.Разработка средств восстановления необнаруженных нарушений зашиты 5.Обоснование технологий необнаруженных нарушений зашиты 6.Оценка ожидаемой эффективности механизмов восстановления	1.Проверка эффективности восстановления необнаруженных нарушений зашиты информации 2.Корректировка проектных решений механизмов восстановления 3.Отладка технологии функционирования механизмов восстановления	1.Обеспечение работы механизмов восстановления 2.Сбор и обработка статических данных о работе 3.Резработка приложений по совершенствованию механизмов восстановления

Анализ содержания таблиц показывает, что репрезентативное множество задач может состоять из некоторого количества классов, каждый из которых включает некоторое количество групп, каждая из которых в свою очередь содержит некоторое количество однородных в функциональном отношении задач.

Классом задач названо однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких функций защиты.

На основе системного и предметного анализа содержания и рациональных путей осуществления функций защиты сформировано 10 классов задач.

Класс 1.1 - введение избыточности элементов системы. Под избыточностью понимается включение в состав элементов системы дополнительных компонентов сверх минимума, который необходим для выполнения ими всего множества своих функций. Избыточные элементы функционируют одновременно с основными, что позволяет создавать системы, устойчивые относительно внешних и внутренних дестабилизирующих воздействий. Различают избыточность организационную (т.е. введение дополнительной численности людей), аппаратную (введение дополнительных технических устройств), программно-алгоритмическую (введение дополнительных алгоритмов и программ), информационную (создание дополнительных информационных массивов), временную (выделение дополнительного времени для проведения обработки информации) и т.п.

Класс 1.2 - резервирование элементов системы. Резервирование, как разновидность задач защиты информации, в некотором смысле противоположно введению избыточности: вместо введения в активную работу дополнительных элементов, наоборот - часть элементов выводится из рау боты и держится в резерве на случай непредвиденных ситуаций. Резервироваться могут практически все элементы ИС, причем различают да

основных вида резервирования, которые получили названия горячего и холодного. Горячим называется такое резервирование, когда выводимые в резерв элементы находятся в рабочем состоянии и способны включат в работу сразу, т.е. без проведения дополнительных операций включен и подготовки; холодным - когда элементы находятся в таком состоянии! что для перевода их в рабочее состояние требуются дополнительные one рации (процедуры).

Класс 1.3 - регулирование доступа к элементам системы. Регулирование доступа, по определению, заключается в том, что доступ на территорию (в помещение, к техническим средствам, к программам, к массивам (базам) данных и т.п.) будет предоставлен лишь при условии предъявления некоторой заранее обусловленной идентифицирующей информации.

Класс 1.4 - регулирование использования элементов системы. Регулирование использования, тоже по определению, заключается в том, что осуществление запрашиваемых процедур (операций) производится лишь при условии предъявления некоторых заранее обусловленных полномочий.

Класс 1.5 - маскировка информации. Заключается в том, что защищаемые данные преобразуются или маскируются таким образом, что преобразованные данные в явном виде могут быть доступными лишь при предъявлении некоторой специальной информации, называемой ключом преобразования.

Класс 1.6 - контроль элементов системы. Данный класс задач предполагает целый ряд проверок: соответствие элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы, состояния существенно значимых параметров внешней среды и т.п.

Класс 1.7 - регистрация сведений. Под регистрацией как классом задач защиты информации понимается фиксация всех тех сведений о фактах, событиях и ситуациях, относящихся к защите информации, которые

возникают в процессе функционирования ИС и знание которых необходимо для эффективной защиты.

Класс 1.8 - уничтожение информации. Под уничтожением как классом задач защиты информации понимается осуществление процедур своевременного уничтожения (или полного вывода из системы обработки) тех элементов информации (или других компонентов системы), которые больше не нужны для функционирования ИС и дальнейшее нахождение которых в ИС может отрицательно сказаться на защищенности информации. Наиболее типичной процедурой данного класса является уничтожение так называемой остаточной информации, т.е. информации, остающейся на регистрах, полях оперативного ЗУ и в других устройствах после решения соответствующей задачи обработки данных в ИС. Ненужной может оказаться информация на отдельных носителях (МЛ, МД), некоторые программные модули, контрольные распечатки, выданные документы и т.п. Одной из разновидностей уничтожения информации является так называемое аварийное уничтожение, осуществляемое при явной угрозе злоумышленного доступа к информации повышенной важности.

Класс 1.9 - сигнализация. Одним из важнейших положений системно-концептуального подхода к защите информации является активность защиты, что обеспечивается созданием функционально самостоятельной системы защиты и осуществлением регулярного управления ее функционированием. Во всякой же системе управления непременно должна быть обратная связь, по которой будет поступать информация (сигналы) о состоянии управляемых объектов и процессов. Процедуры генерирования, передачи и отображения (выдачи) этих сигналов и составляют содержание рассматриваемого класса задач.

Класс 1.10 - реагирование. Вторым важнейшим признаком активности системы защиты является наличие возможностей реагирования на проявление дестабилизирующих факторов с целью предотвращения или, по крайней мере, снижения степени воздействия их на информацию.

Характерным примером такого реагирования может служить противодействие попыткам несанкционированного получения информации злоумышленником, задержание нарушителя и т.п.

Задачи второго вида, т.е. управления механизмами защиты, четко классифицируются в соответствии с функциями управления, поэтому рассматривать их особо нет необходимости.