Лекция 3.1. Методы формирования функции защиты.

1. Определение и анализ понятий функций и задач защиты.

Одно из наиболее фундаментальных положений системно-концептуального подхода к защите информации состоит в том, что предполагается разработка такой концепции, в рамках которой имелись бы (по крайней мере потенциально) возможности гарантированной защиты информации для самого общего случая архитектурного построения АСОД, технологии и условий их функционирования. Системообразующим компонентом концепции, предназначенным для создания таких условий, как это было показано в гл. 1, является множество функций защиты, причем под функцией защиты понимается совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в АСОД различными средствами и методами с целью создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Для того, чтобы множество функций соответствовало своему назначению, оно должно удовлетворять требованию полноты, причем под полнотой множества функций понимается его свойство, состоящее в том, что при надлежащем обеспечении соответствующего уровня (соответствующей степени) осуществления каждой из функций множества гарантировано может быть достигнут требуемый уровень защищенности информации. Именно свойство полноты множества функций служит гарантом достижения требуемой защиты информации. Но отсюда следует, что требование полноты множества функций является абсолютным, и эта полнота должна быть строго доказана.

И еще одно суждение вводного характера относительно функций защиты. В гл. 1 было показано, что защита информации в современных АСОД может быть эффективной лишь в том случае, если она будет осуществляться как непрерывный и управляемый процесс. Для этого должны быть предусмотрены, с одной стороны, механизмы непосредственной защиты информации, а с другой - механизмы управления механизмами непосредственной защиты. Соответственно этому и множество функций защиты должно состоять из двух подмножеств: первого, содержащего функции непосредственной защиты, и второго, содержащего функции управления механизмами защиты.

Обеспечение регулярного осуществления функций защиты достигается тем, что в АСОД регулярно решаются специальные задачи защиты.

При этом задачей зашиты информации называются организованные возможности средств, методов и мероприятий, реализуемых в АСОД с целью

осуществления функций защиты. Основное концептуальное требование к задачам защиты состоит в надежном обеспечении заданного уровня осуществления каждой из полного множества функций защиты. Сущность этого требования заключается в следующем.

Множество функций защиты, как отмечалось выше, должно быть полным в том смысле, что регулярное их осуществление обеспечивает условия для надежной защиты информации в системном плане. При этом варьируя усилиями и ресурсами, вкладываемыми в осуществление различных функций, можно стремиться к такому положению, когда требуемый уровень защиты информации будет достигаться при минимальных затратах, или к положению, когда при заданных затратах будет достигаться максимальный уровень защиты. Иными словами, полнота множества функций защиты и взаимозависимости различных функций создают предпосылки для оптимального построения системы защиты информации в АСОД. Практическая реализация этой возможности может быть обеспечена лишь в том случае, если множество задач защиты будет репрезентативным в том смысле, что будет позволять обеспечивать любой заданный уровень осуществления каждой из функций защиты, и притом с минимизацией расходов на осуществление как каждой функции отдельно, так и их совокупности. Таким образом, задачи защиты информации являются инструментом практической реализации функций защиты в соответствии с объективными потребностями защиты.

Аналогично двум видам функций, очевидно, должны быть предусмотрены и два вида задач защиты: создания и реализации механизмов защиты и управления механизмами защиты. Обоснование перечня, общего содержания и классификации функций и задач защиты рассмотрены в следующих параграфах.

2. Методы формирований функций защиты.

Центральной задачей теории защиты информации является формирование и обоснование полного множества функций защиты, состоящего из двух подмножеств: 1) функции, осуществлением которых создаются условия, необходимые для надежной защиты информации; 2) функции, осуществляемые с целью эффективного использования механизмов защиты при реализации функций первого вида. Для краткости функции первого вида будем называть функциями обеспечения защиты, второго вида - функциями управления механизмами защиты.

Требование полноты множества функций защиты применительно к названным видам интерпретируется следующим образом: множество функций обеспечения защиты должно быть таким, чтобы осуществлением их в различных

комбинациях и с различными усилиями в любой ситуации при функционировании АСОД могли быть созданы все условия, необходимые для надежной защиты информации; множество функций управления должно создавать все предпосылки для оптимальной реализации функций обеспечения в любых условиях.

Акцентируем еще раз внимание на том обстоятельстве, что требование полноты функций защиты является абсолютным в том смысле, что при его нарушении принципы системно-концептуального подхода к защите информации вообще не могут быть реализованы. А, как было показано в гл. 1, надежная защита информации в современных АСОД может быть достигнута только в рамках системно-концептуального подхода.

Вместе с тем принципиально важно подчеркнуть, что регулярных (а тем более формальных) методов решения проблемы формирования полного множества функций защиты не существует (по крайней мере в настоящее время). Вынужденно приходится использовать методы неформальные. Таким образом, формирование функций защиты приходится осуществлять в ситуации, когда требования к формированию являются абсолютными, а методы, которые могут быть при этом использованы, весьма относительны - структурно-логический анализ, экспертные оценки и просто здравый смысл компетентных специалистов.

Совершенно очевидно, что множество функций защиты информации должно быть таким, чтобы надлежащим их осуществлением можно было оказывать желаемое воздействие на любую ситуацию, которая потенциально возможна в процессе организации и обеспечения защиты информации. Следовательно, для формирования полного множества функций прежде всего необходимо выявить и систематизировать полный перечень названных выше ситуаций.

Последовательность и содержание структурно-логического анализа ситуаций, потенциально возможных в процессе защиты информации, можно представить в следующем виде.

Для того, чтобы защищенность информации могла быть нарушена, должны существовать (иметь место) такие условия, при которых могут проявиться дестабилизирующие факторы. Если таких условий не будет, то не будет необходимости в специальной защите информации. Если же потенциальные возможности для проявления дестабилизирующих факторов будут иметь место, то надо оценивать реальную возможность их проявления, обнаруживать факты проявления, принимать меры к предотвращению воздействия их на информацию, обнаружению, локализации и ликвидации последствий этих воздействий. На рис. 12.1 приведена полная структурная схема анализа. Как следует из рисунка, в

зависимости от исходов различных условий, влияющих на анализируемую ситуацию, может быть три различных итоговых события:

Событие №1 - защита информации обеспечена, поскольку даже при условии проявления дестабилизирующих факторов предотвращено их воздействие на защищаемую информацию или ликвидированы последствия такого воздействия.

Событие №2 - защита информации нарушена, поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано.

Событие №3 - защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано.

Защита информации собственно и заключается в создании условий для благоприятного итогового события.

3. Структура полного множества функций защиты.

Очевидно, что множество функций непосредственной защиты информации может быть представлено следующей последовательностью: предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов; предупреждение непосредственного проявления дестабилизирующих факторов в конкретных условиях функционирования АСОД; обнаружение проявившихся дестабилизирующих факторов; предупреждение воздействия дестабилизирующих факторов на защищаемую информацию; обнаружение воздействия дестабилизирую-ших факторов на информацию; локализация (ограничение) воздействия дестабилизирующих факторов на информацию; ликвидация последствий воздействия дестабилизирующих факторов на информацию. Содержание перечисленных функций в общем виде представлено ниже.

Функция №1- предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов. Сущностью данной функции является такое построение архитектуры АСОД, технологических схем автоматизированной обработки информации и их обеспечения, которые сводили бы к минимуму саму возможность появления дестабилизирующих факторов во всех потенциально возможных условиях функционирования АСОД. Иными словами, преследуется упреждающая цель.

Функция №2 - предупреждение непосредственного проявления дестаби-лизирующих факторов в конкретных условиях функционирования АСОД.

Выделением данной функции также преследуется цель упреждения возникновения дестабилизирующих факторов, однако в отличие от предьщущей, мероприятия функции №2 предполагается осуществлять для предупреждения проявления дестабилизирующих факторов в конкретных условиях жизнедеятельности АСОД.

Иными словами - функция №2 является как бы деталировкой функции №1 применительно к конкретным ситуациям, которые потенциально могут иметь место на различных этапах жизненного цикла АСОД.

Функция №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, функция №3 есть функция непрерывного слежения за дестабилизирующими факторами.

Функция №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 предьщущей. Однако осуществление предьщущей 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 функции №4, вообще говоря, должны быть предусмотрены мероприятия по предупреждению воздействия де-стабилизирующих факторов на информацию в любых условиях. С учетом этого обстоятельства функцию предупреждения воздействия целесообразно разделить на две составляющие: предупреждение воздействия на информацию проявившихся и (ДФ - дестабилизирующие факторы) обнаруженных дестабилизирующих факторов (функция 4а) и предупреждение воздействия на информацию проявившихся, но не обнаруженных дестабилизирующих факторов (функция 46).

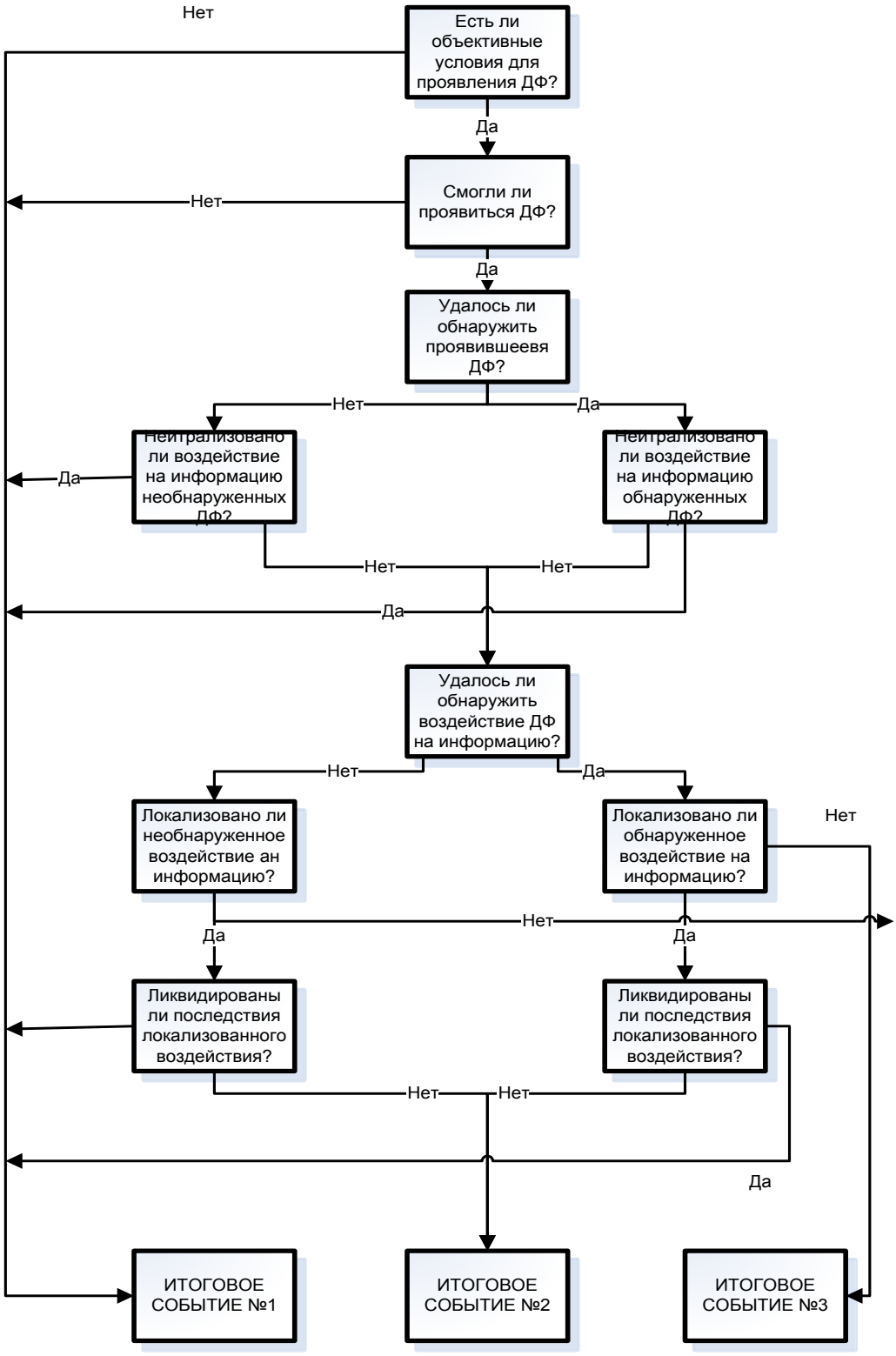

Рисунок 12.1 - Последовательность и содержание анализа ситуаций, потенциально возможных в процессе защиты информации

Функция №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 распространяемая функция есть функция слежения за компонентами защищаемой информации с целью своевременного обнаружения воздействия на них дестабилизирующих факторов. При этом под своевременным понимается такое обнаружение, при котором сохраняются реальные возможности локализации воздействия на информацию.

Функция №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, аналогично тому, как это было отмечено при анализе функции №4, в рамках функции №6 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 составляющие: локализацию обнаруженного воздействия дестабилизирующих факторов на информацию (функция 6а) и локализацию необнаруженного воздействия (функция 66).

Функция № 7 - ликвидация последствий воздействия дестабилизирующих факторов на защищаемую информацию. Под ликвидацией последствий понимается проведение таких мероприятий 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 составляющих: ликвидация последствий обнаруженного и локализованного воздействия дестабилизирующих факторов на защищаемую информацию (функция 7а) и ликвидация последствий локализованного, но не обнаруженного воздействия на информацию (функция 76).

Таким образом, в итоге получаем следующее множество функций непосредственной защиты информации (назовем их функциями первого вида):

1 - предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов;

2 - предупреждение непосредственного проявления дестабилизи
рующих факторов;

3 - обнаружение проявившихся дестабилизирующих факторов;

4а - предупреждение воздействия на информацию проявившихся и обнаруженных дестабилизирующих факторов;

46 - предупреждение воздействия на информацию проявившихся, но необнаруженных дестабилизирующих факторов;

5 - обнаружение воздействия дестабилизирующих факторов на защищаемую информацию;

6а - локализация обнаруженного воздействия дестабилизирующих факторов на информацию;

66 - локализация необнаруженного воздействия дестабилизирующих факторов на информацию;

7а - ликвидация последствий локализованного обнаруженного воздействия на информацию;

76 - ликвидация последствий локализованного необнаруженного воздействия на информацию.

Докажем, что множество перечисленных функций является полным, а именно: надлежащим осуществлением каждой из перечисленных функций можно обеспечить требуемую защиту информации в любых АСОД и в любых условиях их функционирования. Для этого на рис. 12.1 приведены все сочетания событий, которые потенциально возможны при осуществлении всех функций защиты, причем зафиксированы все единичные исходы, которые при этом могут иметь место. Если пронумеровать эти исходы, то нетрудно видеть, что исходы 1 - 6 приводят к итоговому событию №1 - защита обеспечена, исходы 7 и 8 - к итоговому событию №2 -защита нарушена, исходы 9 и 10 - к итоговому событию №3 - защита разрушена.

Каждый из исходов является событием случайным, а все они вместе составляют полную группу несовместных событий. Как известно из теории вероятностей, сумма вероятностей таких событий равна 1.

Лекция 3.2. Содержание полного множества функций защиты.

1. Общая модель исходов при осуществлении функций обеспечения защиты информации.

Докажем, что множество перечисленных функций является полным в том смысле, как это было определено, а именно: надлежащим осуществлением каждой из перечисленных функций можно обеспечить требуемую защиту информации в любых АСОД и в любых условиях их функционирования. Для этого на рис. 13.2 приведены все сочетания событий, которые потенциально возможны при осуществлении всех функций защиты, причем зафиксированы все единичные исходы, которые при этом могут иметь место. Если пронумеровать эти исходы (рис. 13.2), то нетрудно видеть, что исходы 1 - 6 приводят к итоговому событию (см. рис. 13.1) №1 - защита обеспечена, исходы 7 и 8 - к итоговому событию №2 -защита нарушена, исходы 9 и 10 - к итоговому событию №3 - зашита разрушена.

Каждый из исходов является событием случайным, а все они вместе составляют полную группу несовместных событий. Как известно из теории вероятностей, сумма вероятностей таких событий равна 1, Поэтому если через $P_m^{(u)}$ обозначить вероятность m-го исхода, то

$$\sum_{m=1}^{10} P_m^{(u)} = 1 \qquad (13.1)$$

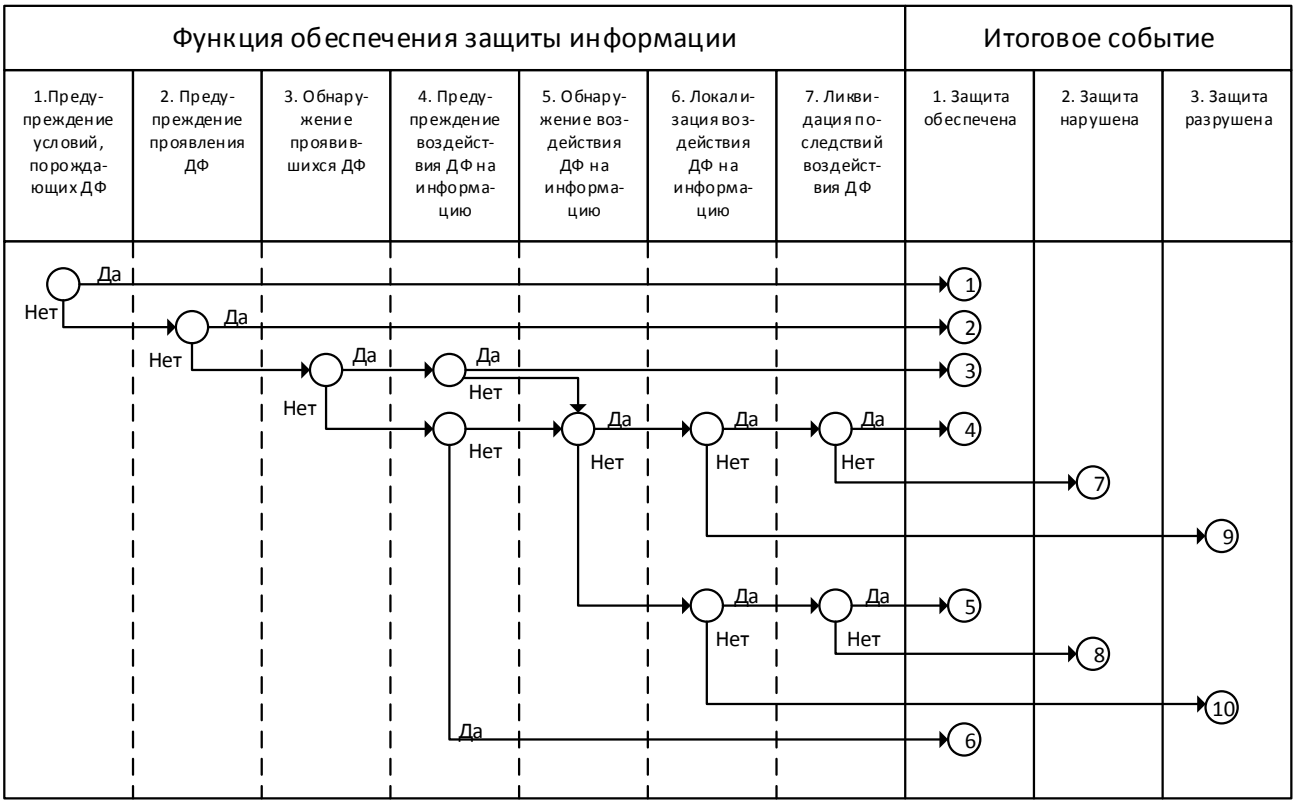

Рисунок 13.1. Общая модель исходов при осуществлении функции обеспечения защиты информации (ДФ дестабилизирующих фактор)

Благоприятными с точки зрения защиты информации являются исходы 1 - 6, поэтому сумма их вероятностей будет не чем иным как вероятностью того, что защищенность информации обеспечена. Если эту вероятность обозначить через *Рз,* то

$$P_з = \sum_{m=1}^{6} P_m^{(u)}.$$

(13.2)

Обозначим через $P_r^{(ф)}$ вероятность успешного осуществления *r*-й функции, тогда для $P_r^{(u)}$ справедливыми будут следующие выражения:

$$P_1^{(u)} = P_1^{(ф)};$$

(13.3)

$$P_2^{(u)} = (1 - P_1^{(ф)}) P_2^{(ф)};$$

(13.4)

$$P_3^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})P_3^{(ф)}P_{4а}^{(ф)};$$
(13.5)

$$P_4^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})P_3^{(ф)}(1 - P_{4а}^{(ф)}) + (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})P_5^{(ф)}P_{6а}^{(ф)}P_{7а}^{(ф)};$$
(13.6)

$$P_5^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})P_3^{(ф)}(1 - P_{4а}^{(ф)}) + (1 - P_3^{(ф)})(1 - P_{4б}^{(ф)})(1 - P_5^{(ф)})P_{6б}^{(ф)}P_{7б}^{(ф)};$$
(13.7)

$$P_6^{(u)} = (1 - P_1^{(ф)})(1 - P_2^{(ф)})(1 - P_3^{(ф)})P_{4б}^{(ф)}.$$
(13.8)

Если выражения (13.3) - (13.8) подставить в (13.2), то в конечном итоге получим

$$P_з = P(\{P_r^{(ф)}\})$$
(13.9)

т.е. защищенность информации целиком и полностью определяется вероятностями успешного осуществления функций защиты.

Поэтому, если требуется обеспечить уровень защищенности информации, равный $\overline{P}_з$, то надо выбрать такие совокупности мероприятий для осуществления каждой из функций защиты, при которых

$$F(\{P_r^{(a)}\}) \geq \overline{P}_з.$$
(13.10)

Таким образом, можно считать доказанной полноту множества функций, но с точностью до того условия, *что* для каждой функции могут быть выбраны необходимые мероприятия.

2. Зависимость уровня осуществления функций защиты от количества расходуемых ресурсов.

Полнота множества функций защиты имеет принципиальное значение еще и с точки зрения создания предпосылок для оптимизации систем защиты информации. Осуществление функций защиты информации сопряжено с расходованием тех или иных ресурсов. Поэтому уровень осуществления каждой из функции защиты при прочих равных условиях будет зависеть от количества расходуемых ресурсов. Если количество ресурсов (например, в

стоимостном выражении), расходуемых на осуществление ***r***-й функции, обозначить через $C_r^{(\phi)}$, то

$$P_r^{(\phi)} = \varphi_r(C_r^{(\phi)}).$$

(13.11)

Тогда зависимость (13.11) можно представить в таком виде:

$$P_з = F\left[\left\{\varphi_r(C_r^{(\phi)})\right\}\right]$$

(13.12)

С учетом этого задачу защиты информации можно сформулировать как оптимизационную, а именно: найти такие ($C_r^{(\phi)}$) при которых выполняются условия:

$$\left.\begin{array}{l} F\left[\left\{\varphi_r(C_r^{(\phi)})\right\}\right] \geq \overline{P}_з; \\ C = \sum\limits_{\forall r} C_r^{(\phi)} \Rightarrow \min \end{array}\right\}$$

(13.13)

или

$$\left.\begin{array}{l} C = \sum\limits_{\forall r} C_r^{(\phi)} \leq \overline{C}; \\ P_з = F\left[\left\{\varphi_r(C_r^{(\phi)})\right\}\right] \Rightarrow \max \end{array}\right\}$$

Здесь $\overline{C}$ - допустимый уровень затрат на защиту информации.

Нетрудно видеть, что первая постановка адекватна тому случаю, когда задаваемый уровень защиты информации в обязательном порядке должен быть достигнут и желательно при минимально возможных затратах, вторая - когда затраты на защиту информации ограничены некоторым уровнем, а естественный желанием при этом является достижение максимально возможного уровня защищенности информации.

В общем случае каждая из функций защиты должна осуществляться в каждой из зон защиты (внешней, контролируемой территории, помещений, ресурсов, баз данных).

Рассмотрим состав и содержание функций второго вида, подлежащих осуществлению в целях управления механизмами защиты информации, обеспечивая высокоэффективное их использование. Состав и содержание

этих функций, а также концепции их осуществления существенно зависят от типа тех систем, для которых они предназначаются.

Системы защиты информации в АСОД относятся к системам организационно-технологического типа, поскольку общую организацию защиты и решение значительной части задач осуществляют люди (организационная составляющая), а защита информации, обрабатываемой с использованием средств электронной вычислительной техники (ЭВТ), осуществляется параллельно с технологическими процессами ее обработки (технологическая составляющая). В общедоступной литературе современные концепции управления в организационно-технологических системах практически не изложены, в силу чего необходимо их кратко рассмотреть.

Основополагающим требованием к управлению в указанных системах на современном этапе выступает требование индустриализации осуществления основных процессов управления. При этом ***под индустриализацией процессов управления*** понимается: *во-первых*, четкое и однозначное формирование состава функций управления; *во-вторых*, разработка и обоснование концептуальных подходов к осуществлению каждой из функций; *в-третьих*, разработка методов, моделей и алгоритмов решения всей совокупности необходимых задач; *в-четвертых*, разработка регулярной технологии решения задач управления в процессе функционирования системы.

Основные аргументы в пользу объективной необходимости индустриализации управления в системах рассматриваемого типа заключается в следующем.

1. Управление в современных условиях стало массовым занятием, в силу чего полностью полагаться лишь на искусство управленца нельзя: технология массового управления непременно должна быть строго регламентированной.

2. Управление на современном этапе является сложным процессом, что обусловлено, с одной стороны, постоянным усложнением управляемых процессов, а с другой - все расширяющейся кооперацией производства. В этих условиях управление должно быть таким, чтобы весь ход производства был строго регламентирован и притом с значительным упреждением во времени.

3. Управление стало высокодинамичным процессом в самом широком толковании этого понятия. Управление высокодинамичными процессами

будет эффективным лишь в том случае, когда содержание процедур управления и правила их выполнения будут строго регламентированы.

4. Управление в современных условиях является высокоответственным процессом, причем как в силу неуклонного роста потерь от некачественного управления, так и в силу того, что нередко приходится управлять объектами и процессами повышенной опасности.

5. В сферу управления интенсивно внедряются средства ЭВТ, управление все больше становится автоматизированным, что предполагает структуризацию соответствующих процессов до уровня представления их в виде алгоритмов.

Применительно к управлению защитой информации в современных АСОД целиком и полностью справедливы все названные выше аргументы, чем и предопределяется настоятельная необходимость в строгой определенности технологии управления.

Научно-методологическим базисом построения названной выше технологии служит так называемая конструктивная теория управления, удовлетворяющая следующей совокупности условий:

1) содержит полный и упорядоченный перечень функций управления;

2) разработана стройная концепция осуществления каждой из функций управления;

3) для каждой процедуры управления разработаны методы ее выполнения для общего случая.

Лекция 3.3. Возможные пути реализации функций обеспечения защиты информации.

1. Определение количества задач для осуществления всех функций защиты во всех зонах защиты.

Для непосредственной организации (построения) и эффективного функционирования комплексной системы защиты информации в АС может быть (а на государственных предприятиях и при больших объемах защищаемой информации - должна быть) создана специальная служба обеспечения безопасности информации (служба компьютерной безопасности).

Служба компьютерной безопасности представляет собой штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее нормального функционирования.

На это подразделение целесообразно возложить решение следующих основных *задач:*

- определение требований к системе защиты информации, ее носителей и процессов обработки, разработка политики безопасности;
- организация мероприятий по реализации принятой политики безопасности, оказание методической помощи и координация работ по созданию и развитию комплексной системы защиты;
- контроль за соблюдением установленных правил безопасной работы в АС, оценка эффективности и достаточности принятых мер и применяемых средств защиты.

Основные функции службы заключаются в следующем:

- формирование требований к системе защиты при создании и развитии АС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования АС;

- обучение пользователей и персонала АС правилам безопасной обработки информации и обслуживания компонентов АС;
- распределение между пользователями необходимых реквизитов доступа к ресурсам АС;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- взаимодействие с ответственными за безопасность информации в подразделениях;
- регламентация действий и контроль за администраторами баз данных,

серверов и сетевых устройств (за сотрудниками, обеспечивающими правильность применения имеющихся в составе ОС, СУБД и т.п. средств разграничения доступа и других средств защиты информации);

• принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты;

• наблюдение за работой системы защиты и ее элементов и организация проверок надежности их функционирования.

Организационно-правовой статус службы обеспечения безопасности информации определяется следующим образом:

• служба должна подчиняться тому лицу, которое несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;

• сотрудники службы должны иметь право доступа во все помещения, где установлены технические средства АС, и право требовать от руководства подразделений прекращения автоматизированной обработки информации при наличии непосредственной угрозы для защищаемой информации;

• руководителю службы защиты должно быть предоставлено право ' запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

• численность службы должна быть достаточной для выполнения всех перечисленных выше функций;

• штатный персонал службы не должен иметь других обязанностей, связанных с функционированием АС;

• сотрудникам службы должны обеспечиваться все условия, необходимые им для выполнения своих функций.

Для решения задач, возложенных на подразделение обеспечения безопасности информации, его сотрудники должны иметь следующие *права:*

• определять необходимость, разрабатывать представлять на согласование и утверждение руководством нормативные и организационно-распорядительные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность сотрудников других подразделений;

• получать необходимую информацию от сотрудников других подразделений по вопросам применения информационных технологий и эксплуатации АС, в части касающейся ОИБ;

• участвовать в проработке технических решений по вопросам ОИБ при проектировании и разработке новых подсистем и комплексов задач (задач);

• участвовать в испытаниях разработанных подсистем и комплексов задач (задач) по вопросам оценки качества реализации требований по ОИБ;

• контролировать деятельность сотрудников других подразделений организации по вопросам ОИБ.

Естественно, все эти задачи не под силу одному человеку, особенно в крупной организации (компании, банке и т.п.). Более того, в службу компьютерной безопасности могут входить сотрудники с разными функциональными обязанностями. В состав такого подразделения должны входить следующие специалисты:

• *руководитель,* непосредственно отвечающий за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информации в АС;

• *аналитики по вопросам компьютерной безопасности,* отвечающие за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем АС и путей обеспечения их защиты, а

также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;

• *администраторы средств защиты, контроля и управления,* отвечающие за сопровождение и администрирование конкретных средств защиты информации и средств анализа защищенности подсистем АС;

• *администраторы криптографических средств защиты,* ответственные за установку, настройку, снятие СКЗИ, генерацию и распределение ключей и т.п.;

• ответственные за решение вопросов защиты информации в разрабатываемых программистами и внедряемых прикладных программах (участвующие в разработке технических заданий по вопросам защиты информации, в выборе средств и методов защиты, участвующие в испытаниях новых прикладных программ с целью проверки выполнения требований по защите и т.д.);

• специалисты по защите информации от утечки по техническим каналам;

• ответственные за организацию конфиденциального (секретного) делопроизводства и др.

2. Возможные пути реализации функций обеспечения защиты информации.

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются технические, организационные и правовые.

Обеспечение безопасности информации — дорогое дело, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Средства зашиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ.

Защита информации является крупномасштабной и весьма сложной проблемой. Естественно, что такой масштабной постановке задачи должна соответствовать не менее масштабная программа реализации функций обеспечения защиты, опирающаяся на развитую инфраструктуру как в масштабах отдельных предприятий и организаций, так и в масштабах государства в целом. Это требует создания разноплановых в функциональном отношении органов защиты, основу системы которых могут составлять отраслевые и территориальные центры защиты информации.

Вся работа сети центров защиты в целях повышения ее эффективности должна координироваться некоторым головным центром, роль которого может выполнять одна из государственных структур, ответственных за обеспечение информационной безопасности России, или их совместное объединение. Головной центр защиты информации должен реализовывать следующие функции:

- организацию и проведение фундаментальных исследований в области защиты информации;

- разработку, формирование и непрерывное совершенствование методологической и инструментальной базы защиты информации;

- научно-методическое и инструментальное обеспечение создания новых территориальных и ведомственных центров защиты;

- научное обоснование организационно-административных решений в области защиты информации;

- оказание текущей повседневной помощи территориальным и ведомственным центрам защиты.

Территориальный или ведомственный центр защиты информации должен представлять собой специализированное научно-производственное предприятие, профессионально ориентированное на разработку, практическую реализацию и внедрение концептуальных решений в области защиты информации, а также конкретных средств, методов и мероприятий защиты. Основные **функции** этих центров защиты могут быть следующими:

- участие в исследованиях и разработках концептуальных вопросов защиты информации;

- аккумулирование новейших достижений в области защиты информации и сведений о разработках методологии, средств и методов защиты;

- приобретение, разработка, накопление и хранение программных и организационных средств защиты;

- формирование, сбор, накопление, систематизация и хранение данных, необходимых для решения центром всей совокупности задач по защите информации;

- оказание абонентам широкого спектра услуг по защите информации;

- сбор, накопление, хранение и аналитико-синтетическая обработка данных о функционировании систем (механизмов) защиты информации у абонентов.

Важное значение для практической реализации концепции комплексной защиты информации имеет также организационно-правовое обеспечение, которое должно представлять собой высокоупорядоченную совокупность организационных решений, законов, нормативов и правил,

регламентирующих общую организацию работ по защите информации, а также создание и функционирование систем защиты информации в конкретных информационных системах. При этом первостепенное значение приобретает разработка типовых документов по защите, основное назначение которых состоит в следующем:

- обеспечение научно-методологического и концептуального единства при решении всех вопросов защиты информации;

- создание условий для однозначного понимания и для практической реализации основных положений концепции защиты информации;

- обеспечение необходимыми методиками и данными всех органов и лиц, участвующих в решении вопросов защиты информации;

- обеспечение нормативно-правового регулирования процессов защиты информации.

Все документы должны образовывать единую систему, основными группами которой являются: справочно-информационные документы, стандарты, руководящие методические материалы, инструкции.

К группе справочно-информационных относятся также документы, которые в систематизированном виде содержат полную совокупность сведений, необходимых и достаточных, с одной стороны, для получения четкого и однозначного представления обо всех аспектах проблемы защиты, а с другой - признающихся большинством специалистов-профессионалов в области защиты информации.

К группе стандартов, естественно, относятся такие документы, которые являются образцом, эталоном в смысле совершенства по всем основным параметрам, имеют по ним точный сертификат и утверждены полномочным органом.

К руководящим методическим материалам по установившейся практике относится совокупность документов, содержащих полное и систематизированное описание соответствующих вопросов, относящихся к защите информации и утвержденных полномочными органами (однако, в отличие от стандартов, утверждение носит лишь рекомендательный характер).

К инструкциям отнесены систематизированные наборы типовых инструкций для различных категорий подразделений и лиц, имеющих отношение к защите информации.