ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ СИСТЕМАХ ПЕРЕДАЧИ И ОБРАБОТКИ ДАННЫХ

Есиков О.В., Кислицин А.С.
Тульский артиллерийский инженерный институт
300012, Тула, пр.Ленина 99, кафедра “Математического программного и информационного обеспечения АСУ”
Закрытое акционерное общество «ЛУКОЙЛ-ИНФОРМ»
101000, Москва, Сретенский бульвар 11

Рассмотрены особенности комплексного подхода к построению систем защиты информации в современных системах передачи и обработки данных. Сформулированы требования к комплексным системам защиты. Для обеспечения выполнения данных требований предлагается многоуровневое построение комплексной системы защиты.

Современные системы передачи и обработки данных (СПОД) отличаются территориальной распределенностью, неоднородностью составляющих их компонентов, интегрированностью в глобальные сети. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успешного выполнения поставленных задач в любой системе СПОД. В этих условиях резко обостряется ситуация с защитой информации в данных системах.

Защищенность информации будет обеспечена, если будут созданы такие условия, при которых будет иметь место одно из следующих событий.

1. Дестабилизирующие факторы, следствием проявления которых может быть нарушение защищенности информации, вообще не могут проявиться.
2. Дестабилизирующие факторы, даже проявившись, не смогут воздействовать на информацию.
3. Воздействие на информацию даже если оно произойдет будет своевременно обнаружено, локализовано и устранено.

Учитывая многообразие потенциальных угроз информации в СПОД, сложность их структуры и функций, а также участие человека в технологическом процессе обработки информации, цели защиты информации могут быть достигнуты только путем создания системы защиты информации на основе комплексного подхода [1]. Данный вывод становится особенно важным в связи с тем, что в последнее время становится все более очевидным – защищать необходимо не только информацию, содержащую государственную или военную тайну, но и информацию, содержащую промышленные и коммерческие секреты.

Система защиты информации должна строиться на основе данных о структуре системы передачи и обработки данных и плане построения информационно-вычислительного процесса. При этом процедуры и механизмы защиты информации должны планироваться к использованию на всех этапах жизненного цикла СПОД.

Комплексный подход к построению системы защиты ориентирован на создание защищенной среды обработки информации в СПОД, объединяющей в единый комплекс разнородные средства защиты информации, образующие комплексную систему защиты. Комплексность системы защиты информации достигается охватом всех возможных угроз и согласованием между собой разнородных методов и средств, обеспечивающих защиту всех элементов СПОД.

Исходя из того, что комплексная система защиты информации является интегрированной со всеми элементами СПОД и процессами обработки информации, к ней должны предъявляться следующие требования:

1. система защиты информации должна обеспечивать выполнение СПОД своих основных функций без существенного ухудшения характеристик последней;
2. она должна быть экономически целесообразной, так как стоимость системы защиты информации включается в стоимость СПОД;
3. защита информации в СПОД должна обеспечиваться на всех этапах жизненного цикла, при всех технологических режимах обработки информации, в том числе при проведении ремонтных и регламентных работ;
4. в систему защиты информации должны быть заложены возможности ее совершенствования и развития в соответствии с условиями эксплуатации и конфигурации СПОД;
5. она в соответствии с установленными правилами должна обеспечивать разграничение доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию, т.е. обладать свойствами активной и пассивной защиты;
6. при взаимодействии защищаемой СПОД с незащищенными СПОД система защиты должна обеспечивать соблюдение установленных правил разграничения доступа;
7. система защиты должна позволять проводить учет и расследование случаев нарушения безопасности информации в СПОД;
8. применение системы защиты не должно ухудшать экологическую обстановку, не быть сложной для пользователя, не вызывать психологического противодействия и желания обойтись без нее.

В случае комплексного применения средств и методов защиты информации, основная задача защитных систем состоит не в абсолютной неприступности, а в невозможности для взломщиков получить

доступ к закрытой информации за разумный срок или разумные деньги. При этом, механизмы системы защиты должны функционировать достаточно эффективно даже в том случае, если их структура и содержание известны злоумышленнику.

Последовательность действий по построению комплексной системы защиты информации от деятельности злоумышленников должна включать в себя следующие шаги.

1. Анализ возможных целей злоумышленника и прогноз ущерба от их реализации.
2. Детализация и доуточнение целей злоумышленника. Выделение перечня угроз информации реализуемых злоумышленником для достижения своих целей и построения перечня средств и методов защиты информации, нейтрализующих эти угрозы.
3. Построение моделей возможных действий злоумышленника по достижению своих целей.
4. Составление наиболее полного перечня средств защиты – претендентов на включение в состав комплекса средств защиты. Выбор состава комплекса средств защиты информации.

В следствие того, что действия человека не возможно заранее и строго определенно спрогнозировать, математическая модель деятельности злоумышленника может быть разработана на основе использования вероятностного критерия эффективности.

Для обеспечения выполнения требований, предъявляемых к комплексной системе защиты, а также снижения размерности соотвествующих задач оптимизации, ее целесообразно строить по многоуровневой схеме. Подобное ее построение позволяет комплексно использовать различные средства и методы защиты, и за счет этого повысить общую эффективность системы в целом при снижении расходов на ее организацию и обслуживание [2].

Уровни системы защиты выделяются исходя из:

1. территориальной локализованности объектов защиты;

2. характерных особенностей защищаемых обеъктов;

3. противодействию определенной совокупности угроз (например, проникновение на охраняемую территрорию).

Каждый уровень системы защиты может в свою очередь делиться на ряд рубежей или эшелонов, функционирующих в тесной взаимосвязи. Каждый рубеж строится на основе одного или совокупности средств защиты, объединяющихся по принципу противодействия конкретной угрозе (например, проникновению нарушителя в охраняемое помещение) или единообразием принципа действия. Все рубежи защиты должны иметь относительно одинаковую степень защищенности в соответствии со степенью угроз объекту защиты, что позволяет эффективно распределить ресурсы системы защиты по уровням и рубежам. То есть большей по уровню угрозе должна соответствовать большая по эффективности совокупность средств защиты, и наоборот. Кроме этого, объем принимаемых мер безопасности должен соответствовать уровню существующих и потенциальных угроз информации, в противном случае система защиты будет экономически неэффективной. Для предотвращения возможности обхода или разрушения отдельных элементов системы защиты каждое предпринимаемое защитное мероприятие должно обеспечиваться в свою очередь защитой.

Выбор состава комплексов средств защиты может быть осуществлен решением оптимизационной задачи сформулированной на основе построенных моделей действий злоумышленника.

Литература

1. Есиков О.В. Математическая модель оптимизации состава комплекса средств защиты информации современных автоматизированных систем обработки данных// Приборы и системы. Управление, контроль, диагностика. № 4, 2000

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.:Кн.1.-М.:Энергоатомиздат, 1994.-400с.

PRINCIPLES OF CONSTRUCTING INFORMATION PROTECTION SYSTEMS IN UP-TO-DATE DATA TRANSMISSION AND PROCESSING SYSTEMS

Esikov O.V., Kislitsin A.S.

The Tula Artillery Engineering Institute
300012, Tula, Prospect Lenina 99, Chair of "Mathematical Code and Information Support for Computer-Aided Control Systems"
Closed Stock Company LUKOIL-INFORM, 101 000, Moscow, 11 Sretensky br.

The paper considers specific features of a complex approach to construction of information protection systems in up-to-date data transmission and processing systems. Requirements to complex protection systems are formulated. Multi-level construction of a complex protection system is proposed to ensure observation of the above requirements.

The up-to-date data transmission and processing systems (DTPS) are characterized by territorial distributivity, non-uniformity of their components and the degree of integration into global networks. Availability of information of a required quality in due time and at a required place is a pledge of successful implementation of the tasks set up for any DTPS system. Under such conditions the situation with information protection in the given systems becomes strongly aggravated.

The information will be protection provided the conditions under which one of the below events occurs are created.

1. The destabilizing factors of which the consequences may result in destruction of the information protection, cannot occur in general.
2. The destabilizing factors even if occurring cannot affect the information.
3. An effect on the information, even if it occurs, will timely be identified, localized and eliminated.

Under current conditions of DTPS functioning the purposes of the information protection can be achieved by way of creating a system for information protection based on a complex approach only [1]. This conclusion becomes especially important for it lately comes more and more obvious that it is necessary to protect not only the information containing State or military secrets but also the information containing industrial and commercial secrets.

Construction of the information protection system should be based upon the data on the information transmission and processing system structure and upon the program on building the information and computation process. In this case, the information protection procedure and mechanisms should be planned for application at all steps of the DTPS life cycle.

The complex approach to the protection system construction is directed toward creating a protected environment for information processing in DTPS which combines diverse information protection means, constituting a complex protection system, into a single protection system. The complex character of the information protection system is attained by covering all possible menaces and by mutual coordination of all diverse techniques and means ensuring protection of all the DTPS components.

The following requirements should be made with regard to the complex information protection system proceeding from the fact that it is integrated with all the DTPS components and the information processing processes:

1. the information protection system should provide a possibility for DTPS to implement its basic functions without substantial deterioration of its performances;
2. it should be expedient from the economic viewpoint;
3. the information protection in DTPS should be provided at all steps of the life cycle, in all information processing modes, among those during repair and maintenance;
4. the information protection system should envisage possibilities of its further updating and development;
5. it should have active and passive protection properties;
6. the protection system should provide observation of the separated access rules in the course of interaction between protected and unprotected DTPS systems;
7. the protection system should make it possible to perform registration and investigation of the events related to information safety infringement in DTPS;
8. the protection system application should not deteriorate ecological environment, should not be complicated for user, it should not cause psychological counteraction and desire to avoid its using.

In case of combined application of the information protection means and techniques, the principle purpose of the protection systems is not an absolute inaccessibility but it should make impossible for an intruder to get an access to classified information during a reasonable time and for reasonable money. For this purpose, functioning of the protection system mechanisms should be efficient enough even if their structure and content are known to the intruder.

The sequence of actions aimed at constructing a complex system for protecting information against intruder's actions should comprise the following steps.

1. Analysis of intruder's probable aims and prognosis on a detriment due to their realization.
2. Working out in detail and specifying the intruder's aims. Identification of a list of menaces to the information possible for the intruder to realize for attaining his aims, and production of a list of the information protection means and techniques to neutralize the above menaces.
3. Constructing models of the intruder's possible actions aimed at attaining his aims.

4. Producing a most complete list of protection means as pretenders for inclusion into a complex of protection means. Determination of the content of the information protection means complex.

A mathematical model of the intruder's actions is possible for elaboration based on application of the probabilistic criterion of efficiency since actions of a man are impossible to forecast in advance and in a strictly determined manner.

In order to ensure observation of the requirements made to the complex protection system and also reduce dimensions of optimization tasks, it is expedient to construct it following the multi-level scheme. Such a construction allows for various protection means and techniques to be used in a complex manner and, on account of this, to increase the total efficiency of the system as a whole and at the same time to reduce expenditures for its organization and maintenance [2].

Each level of the protection system may, in its turn, be subdivided into a number of boundaries or echelons functioning in close interaction. Each boundary is constructed on the basis of one or a set of protection means to be combined together proceeding from the principle of counteraction with regard to a certain menace (e.g. penetration of an intruder into a room under guard) or uniformity of an action principle. All protection boundaries should have a relatively equal degree of protection in accordance with the degree of menaces to the object of protection that allows the resources of a protection system to be distributed by levels and boundaries. The scope of safety measures to be undertaken should be consistent with the level of existing and potential menaces to the information. Each protection measure undertaken should , in its turn, be provided with protection to prevent possible bypassing or destruction of the system separate components.

The choice of content of the protection means complexes can be made by solving an optimization task formulated on the basis of a model for an intruder's actions.

REFERENCES:

1. O.V.Esikov, Mathematical Model of Content Optimization for a Complex of Information Protection Means in Up-to-Date Computer-Aided Data Processing Systems// Instrumentation and Systems. Control, Monitoring, Diagnostics, # 4, 2000
2. V.A.Gerasimenko, Information Protection in Computer-Aided Data Protection Systems. In 2 vol. Volume 1, -N.: Energoatomizdat, 1994.-400p.