УДК 316.776; +34; +62; +65.012.8

ОБЩАЯ ПАРАДИГМА ЗАЩИТЫ ИНФОРМАЦИИ

Павел Орлов, Игорь Громыко, Виталий Носов, Николай Логвиненко, Елена Громыко*

*Национальный университет внутренних дел, *Харьковская облгосадминистрация*

Анотація: **Сформульована загальна парадигма захисту інформації з метою створення теоретико-методологічних основ забезпечення безпеки інформації.**

Summary: **The general paradigm of protection of the information is formulated for creation of theoretical and methodological bases a safety of the information.**

Ключевые слова: **Парадигма, защита информации, теоретические основы.**

Введение

В рамках государственной политики обеспечения безопасности информационных ресурсов на сегодняшний день остро требуется создание и развитие методологии эффективного обеспечения безопасности информации. Для этого необходимо решить ряд комплексных задач [1]:

- обоснование понятийного аппарата;
- аналитико-синтетическая обработка имеющихся данных;
- обоснование современной постановки задач;
- обоснование стратегических подходов к обеспечению безопасности;
- разработка методов решения задач обеспечения информационной безопасности;
- обоснование структуры и содержания инструментально-методологической базы решения задач;
- определение задач обеспечения безопасности, путей и способов их решения;
- обоснование направлений развития теории и практики обеспечения безопасности информации.

С целью создания теоретико-методологических основ обеспечения безопасности информации авторами данной статьи была предпринята попытка определить суть процесса защиты информации путем формулировки ОБЩЕЙ ПАРАДИГМЫ ЗАЩИТЫ ИНФОРМАЦИИ через термины, значение которых общеприняты или определены в различных источниках. Для некоторых терминов была дана авторская трактовка, исключившая определение этих терминов через самих себя.

Изначально приведем определение понятия "парадигмы". **Парадигма** это исходная концептуальная схема, модель постановки проблем и их решения, методов исследования, господствующих в течении определенного исторического периода в научном сообществе [2].

Основная часть

На сегодняшний день существует несколько сотен вариантов определения сущности термина "информация". В данной работе мы исходим из того, что **информация –** *это зафиксированное на носителе представление о предметах, процессах, событиях, природных явлениях и прочее*.

Под **фиксацией** (от лат. fixus – прочный, закреплённый) понимается закрепление чего-либо в определённом положении или виде. Например, в письменном виде сведений, мыслей [2]. Информация для своего существования всегда требует наличия **носителя.**

При этом в качестве **носителя** информации может выступать поле или вещество. В некоторых случаях в качестве **носителя** информации может рассматриваться человек [3]. В процессе информационных отношений носители могут быть **носителями-источниками** (**источниками**) или **носителями-получателями** (**получателями**) в зависимости от направления перемещения информации. В законе Украины "Про информацию" под **источниками** информации понимаются предусмотренные или установленные Законом носители информации: документы или другие носители информации, которые представляют собой материальные объекты, сохраняющие информацию [4]. В общем случае **получатели воспринимают** информацию через сенсор (датчик, измерительный преобразователь). Процесс **восприятия** весьма сложен, и состоит из процессов приёма и преобразования информации, обеспечивающих отражение объективной реальности и ориентировку в окружающем мире. Восприятие может включать в себя [2]:

- обнаружение объекта в поле восприятия;
- различение отдельных признаков в объекте;
- выделение в нём информативного содержания, адекватного цели действия;
- формирование образа восприятия.

В определении термина "информация" под **представлением** понимается образ или сущность предмета, процесса, события, природного явления (и пр.), воспринятые датчиками приборов или непосредственно органами чувств, а также созданные продуктивным (воссоздающим и творческим) *воображением*

представителей животного мира или элементами искусственного интеллекта различных устройств, где **воображение** – это психическая деятельность, состоящая в создании представлений и мысленных ситуаций, никогда в целом не воспринимавшихся человеком в действительности. Различают воссоздающее и творческое воображение [2].

Проведенные исследования дают основания утверждать, что

ИНФОРМАЦИЯ СЧИТАЕТСЯ ЗАЩИЩЕННОЙ, ЕСЛИ ПРИ ЕЕ ПЕРЕМЕЩЕНИИ СОБЛЮДАЕТСЯ РЕЖИМНАЯ АДЕКВАТНОСТЬ КОММУНИКАБЕЛЬНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ.

Нарушение информационной безопасности возможно лишь при перемещении информации. Например, при несанкционированном ознакомлении (чтении) документа с бумажного носителя происходит перемещение (копирование) информации в мозг человека, который является носителем-получателем информации [3]. В формулировке парадигмы **перемещение информации** – это изменение пространственных координат носителей информации или уничтожение информации с сохранением (разрушением) носителя.

В процессе перемещения информации может происходить смена ее носителя. Например, носителями информации при ее перемещении могут быть:

- материальные среды (воздух, вода, металл и пр.);
- сенсоры или датчики;
- преобразователи и другие объекты живой и неживой природы, несущие функцию **промежуточных носителей информации**.

В формулировке парадигмы использовано понятие "режимная адекватность", состоящее из терминов "режим" и "адекватность". **Режим** это совокупность норм для достижения какой-либо цели [2], например, для защиты информации. Здесь обязательно учитывается **режим доступа к информации,** как предусмотренный правовыми нормами порядок получения, использования, распространения и хранения информации [4]. **Адекватность** (от лат. adaequatus – приравненный, равный) – это соответствующее, верное, точное.

Следующее понятие, которое использовано в парадигме - **коммуникабельность** (от позднелатинского – communicabilis – соединимый, сообщающийся). Коммуникабельность означает совместимость (способность к совместной работе) разнотипных систем передачи информации (например, в электросвязи – аналоговых и дискретных, в телевидении – с различным числом строк разложения телевизионного кадра), способность к общению, общительность [2].

Раскроем смысловое значение составных частей парадигмы.

Режимная адекватность носителей информации – это соответствие режимов доступа носителей информации (источника и получателя) при их взаимодействии.

*Пример режимной неадекватности***:** ознакомление с содержимым секретного документа без права на доступ к секретной информации.

*Пример режимной адекватности***:** личный разговор двух людей, желающих передать и соответственно получить информацию с ограниченным доступом, и являющуюся собственностью одного из них.

Коммуникабельные носители информации – это носители информации, способные к взаимодействию.

*Пример некоммуникабельности носителей***:** через сенсор – органы зрения (глаза) человек не способен воспринять речевую (акустическую) информацию.

*Пример коммуникабельности носителей***:** через сенсор – органы зрения (глаза) человек способен воспринять информацию, зафиксированную на бумажном носителе на понятном для него языке.

Промежуточные носители информации, также как и носитель-источник и носитель-получатель, должны соответствовать требованиям режимной адекватности и коммуникабельности.

Режимная адекватность коммуникабельных носителей информации – это способность носителей информации участвовать в информационном обмене при соответствии режимов доступа.

Представляется важным рассмотреть парадигму через призму ее дееспособности при наличии основных информационных угроз.

В общем случае под информационной **угрозой** понимается потенциальное нарушение безопасности или степень вероятности возникновения такого явления (события), следствием которого могут быть нежелательные воздействия на информацию.

Из множества способов классификации угроз информации наиболее общей является их классификация по результатам возможного влияния на информацию [3]:

- угрозы нарушения конфиденциальности;
- угрозы нарушения целостности;
- угрозы нарушения доступности.

Угрозы **конфиденциальности** направлены на запрещенное режимом доступа перемещение информации от носителя-источника к носителю-получателю.

Информация сохраняет конфиденциальность, если соблюдается, прежде всего, согласно сформулированной парадигме, режимная адекватность носителей информации.

Угрозы **целостности** информации направлены на запрещенное режимом доступа (порядка получения, использования, распространения и хранения информации) ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно, а также в результате объективных воздействий со стороны среды, окружающей носитель информации.

Информация сохраняет целостность, если соблюдаются, в соответствии со сформулированной парадигмой, установленная режимная адекватность относительно правил ее модификации (удаления).

Любой субъект, воздействующий на носитель-источник информации с целью модификации информации, можно рассматривать как **носитель** информации, несущей в себе представление о необходимой модификации (удалении) информации носителя-источника информации. В процессе модификации происходит перемещение модифицирующей информации.

Воздействие объектов, процессов, окружающей среды и других факторов, которые часто относят к разряду "случайных" – это несоответствие носителя-источника информации установленному режиму доступа, часто приводящее к нарушению коммуникабельности. Данное воздействие является нарушением режимной адекватности, как следствие, коммуникабельности носителей информации.

Угрозы **доступности** (отказ в обслуживании) направлены на преднамеренное или непреднамеренное нарушение коммуникабельности носителей информации при их взаимодействии. Нарушение коммуникабельности прерывает разрешенные режимом доступа процессы перемещения информации.

Информация сохраняет доступность, если сохраняется коммуникабельность носителей информации при их взаимодействии.

Выводы

Сформулированная парадигма (которая может интерпретироваться как общий закон, аксиома или основное правило) выносится на обсуждение с целью проверки ее на соответствие всем современным аспектам информационной безопасности.

В случае успешной апробации данная парадигма может стать краеугольным камнем, вокруг которой возможно построение и эффективное развитие теоретико-методологических основ обеспечения безопасности информации, основное содержание которых приведено во введении к данной статье. В первую очередь видится необходимость переработки нормативно-методической базы, касающейся информационной безопасности, а потом и коррекция созданных и построение новых комплексных систем защиты информации.

Авторы ждут отзывов, критических замечаний и рекомендаций от всех заинтересованных лиц и организаций.

Литература: 1. Безопасность информационных технологий. Методология создания систем защиты/ В. В. Домарев. – К.: ООО "ТИД "ДС", 2001. – 688 с. 2. Советский энциклопедический словарь/ Гл. ред. А. М. Прохоров 4-е изд. – М.: Сов. энциклопедия, 1989, – 1632 с. 3. НД ТЗИ 1.1 – 002 – 99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Нормативный документ ДСТЗИ СБ Украины. Киев, 1999. 4. Закон України "Про інформацію" № 2657–XII від 02. 10. 92р.

УДК 002.6+342.7

ДЕЯКІ ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ВЗАЄМОВІДНОСИН ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Гурковський

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Анотація: **Пропонуються організаційно-правові заходи щодо координації боротьби з комп'ютерними правопорушеннями.**