Синергетические аспекты интеграции современных способов защиты каналов передачи данных в условиях информационного противоборства

Synergetic aspects of integration of modern protection methods for data communication channels in the conditions of information confrontation

Кежаев / Kezhaev V.
Валерий Алексеевич
(kezhov@rambler.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Михайловская военная артиллерийская академия» МО РФ,
профессор.
г. Санкт-Петербург

Николаев / Nikolaev G.
Геннадий Александрович
(an-33@rambler.ru)
ФГКВОУ ВО «Военная академия Генерального штаба ВС РФ»,
начальник управления Военного института (управления национальной обороной).
г. Москва

Ключевые слова: защита информации – information protection; канал передачи данных – data communication channel; синергетический эффект – synergetic effect; информационное противоборство – information confrontation; информационный ресурс – information resource.

Приведен краткий анализ проблем, связанных с необходимостью защиты информационных систем специального назначения. Классифицированы наиболее характерные угрозы, способные нарушить устойчивую работу каналов передачи данных. Обоснованы перспективные направления реализации их защиты в современных условиях. Предложено объединить возможности различных способов защиты с целью получения синергетического эффекта, позволяющего повысить эффективность защиты каналов передачи данных в условиях информационного противоборства.

The article gives brief analysis of problems connected with the requirement for protection of special purpose information systems. The most specific threats which can disturb stable operation of data communication channels are categorized. Promising trends of implementation of their protection in modern conditions are substantiated. It is proposed to combine capabilities of different methods of protection with the purpose of receipt of synergetic effect which allows to increase the efficiency of protection of data communication channels in the conditions of information confrontation.

В процессе применения информационных систем специального назначения (автоматизированных систем, относящихся к классу эргатических систем, предназначенных для управления в условиях противоборства сторон с антагонистическими целями) возникают проблемы, связанные с необходимостью защиты каналов передачи данных. Эти проблемы приобретают особую актуальность в условиях информационного противоборства, характерного для современной эпохи. В свою очередь, их возникновение обусловлено наличием постоянной угрозы перехвата, подмены, злонамеренного разрушения информационных массивов, неправомочной имитации прав соответствующих должностных лиц органов управления и т.д. [1]. При этом наибольшую опасность представляют попытки несанкционированного вмешательства в функционирование информационных систем специального назначения, атаки на каналы передачи данных, по которым в систему доставляется вся необходимая информация. Такое вмешательство в настоящее время носит, как правило, агрессивный деструктивный характер, поскольку разрушается вся система управления.

Анализируя результаты известных атак на информационные системы специального назначения [2, 3], можно выделить следующие виды угроз по возрастанию степени их опасности (таблица 1):

Следует иметь в виду, что опасность для работоспособности информационных систем специального назначения, возникающая из-за ошибок персонала, основывается на той или иной степени алгоритмической уязвимости программного обеспечения от неверных действий пользователей и может приводить к сбоям систем. Как следует из содержательной части этой опасности, ее можно существенно снизить, повысив уровень подготовки обслуживающего персонала, качество программного обеспечения и т.д. Поэтому влияние такой опасности можно заранее прогнозировать и принять соответствующие меры защиты.

Более сложно защититься от атак со стороны хакеров. Дело в том, что в основе хакерской деятельность лежит высокая степень понимания процессов, протекающих в информационных системах. Поэтому уровень опасности от их действий, направленных на нарушение систем защиты информации, на нелегальное использование информационных ресурсов потенциально очень велик. Об опасности подобных атак свидетельствуют,

Таблица 1

Примерный перечень наиболее характерных угроз для каналов передачи данных

№ п.п.	Наименование типовых угроз	Наиболее характерный период возникновения угрозы	
		мирное время	время конфликта
1	Ошибки персонала, обрабатывающего информацию, вызванные их недостаточным уровнем подготовки или стрессовой ситуацией	+	+
2	Деструктивная деятельность хакеров	+	
3	Сознательные деструктивные действия со стороны неудовлетворенных своим положением сотрудников, обслуживающих информационные системы специального назначения	+	
4	Инициативный шпионаж	+	
5	Преднамеренные попытки завладеть ценной информацией, исказить ее, либо подменить на ложную	+	+
6	Локальные действия и системные атаки с целью разрушения структурированных информационных массивов систем управления в ходе информационного противоборства		+

например, сообщения американской печати о взломе таких, казалось бы, хорошо защищенных систем, как:

компьютерные сети Ливерморской ядерной лаборатории;

Баллистической лаборатории армии США в Абердине;

исследовательского центра и центра управления NASA и других значительных правительственных и частных организаций.

Другим подтверждением степени опасности этой угрозы являются следующие факты, приведенные в одном из исследований Group IB. В 2010 г. киберпреступники по всему миру выкачали из легального бизнеса и интернет-пользователей 7 млрд долларов. Доля россиян и жителей СНГ составила почти треть от этой суммы – 2,5 млрд долларов. В 2011 г. преступники с пространства бывшего СССР получили около 3,7 млрд долларов, а в 2013 г. удвоили этот показатель.

Следующим источником опасности являются сотрудники, обслуживающие информационные системы специального назначения, которые тем не менее в силу ряда причин готовы и способны нанести ущерб этим системам. Именно они, в свою очередь, участвуют в формировании внутренней угрозы. Высокий уровень опасности в данном случае обусловлен тем, что должностные лица из числа обслуживающего персонала имеют легальный доступ к информационным ресурсам системы. Для реализации имеющихся мотивов они чаще всего используют удаление важной информации, сознательное заражение информационной системы компьютерными вирусами, а иногда и переход к инициативному шпионажу. Данная угроза, несомненно, актуальна из-за исключительной напряженности информационного противоборства в современном мире.

Инициативный шпионаж чаще всего связан с угрозой, также исходящей от персонала. В целом он менее опасен, чем целенаправленный шпионаж иностранных государств. Однако при наличии просчетов в системах защиты информации и в мероприятиях органов специальной защиты может служить источником крупных неприятностей, связанных с разглашением государственной тайны.

Опыт конфликтов в современном мире свидетельствует, что различные группы с помощью информационных систем, особенно террористического характера, стараются придать своим акциям большее значение, запугать население, посеять панику, шантажировать противодействующие им государственные органы.

Действия иностранных разведок направлены на сбор информации, циркулирующей в автоматизированных системах управления. Но в случае успешных попыток в отношении информационных систем специального назначения эти действия особенно опасны из-за высокой степени концентрации собираемой информации. При этом, как показывают события современности, отмечаются небезуспешные попытки использования для этих целей хакеров.

Самой серьезной угрозой для информационных систем специального назначения являются удары, наносимые в рамках информационного противоборства. В

некоторых ситуациях, как отмечают специалисты, по степени ущерба, нанесенного государству и обществу в целом, ущерб может быть сопоставим с результатами ядерной войны. Данный ущерб будет являться результатом мероприятий глобального характера, направленных на разрушение информационного пространства государства. В этом случае может произойти полное разрушение систем управления государством, экономикой и национальной обороной. На начальном этапе информационного противоборства могут наноситься локальные информационные удары с целью вывода из строя систем управления первичного звена. В этих целях могут использоваться боевые вирусы и «логические управляемые мины». Кроме традиционных каналов распространения, боевые вирусы могут передаваться по радиоканалам во время тактических действий и иметь форму «троянского коня» – информационной дистанционно-управляемой мины.

По мнению американских специалистов, именно система управления первичного звена является наиболее восприимчивой к вирусам такого рода. Кстати, впервые эта угроза заявила о себе в апреле 1990 года перед операцией «Буря в пустыне». В этот период было обнаружено, что несколько тысяч армейских компьютеров инфицировано вирусами «Иерусалим», «Иерусалим-В» и «Булыжник». Как оказалось, вирусы были внедрены при использовании полевых компьютеров для таких игр как «Solitaire». Во время проведения боевых операций эти вирусы могли бы серьезно повлиять на боеспособность войск, эффективность боевых действий и в конечном итоге на исход операции.

К сожалению, общим негативным фоном, не способствующим повышению защищенности и устойчивости информационных систем специального назначения, остается недостаточное внимание к решению проблем в этой области. Например, даже в армии США из-за сокращения военного бюджета министерства обороны в свое время были вынуждены отказаться от обновления операционной среды на основе UNIX–систем. Вместо этого был осуществлен постепенный переход в некритичных областях на семейство MS Windows NT, значительно уменьшающее как первичные затраты на приобретение, так и на стоимость владения.

При этом, конечно, учитывалось, что по своей сути семейство MS Windows NT разрабатывалось для обеспечения коммерческих приложений в наиболее ответственных областях, а также для поддержки научно-технических расчетов и компьютерного проектирования.

Таблица 2

Типовые ситуации, демонстрирующие снижение уровня опасности информационных атак на каналы передачи данныхв зависимости от степени интеграции способов защиты

№ п.п.	Характеристика типовых ситуаций, усложняющих реализацию процедур защиты	Экспертная оценка численного значения вероятности защиты информации в канале передачи данных
1	Расширение диапазона действия поражающих факторов перспективных видов информационного противоборства	0,3 / 0,7
2	Возрастающая сложность и распределенность компьютерных сетей информационных систем специального назначения	0,1 / 0,9
3	Высокий динамизм условий эксплуатации каналов передачи данных, обусловливающий необходимость периодического изменения топологии сети и аппаратной основы самих каналов	0,2 / 0,8
4	Переход на обработку информации в рабочих станциях, использующих достаточно известные Intel–платформы	0,4 / 0,6
5	Передача данных на основе типовых, хорошо изученных протоколов TCP/IP и им подобных	0,4 / 0,6

Примечание: в числителе указана оценка, относящаяся к отдельному способу защиты информации, а в знаменателе – к интеграции различных способов в единый комплекс.

Поэтому оно не в полной мере отвечало требованиям к системам военного назначения, хотя корпорация Microsoft и обещала довести его до соответствующего уровня. Весьма красноречивым фактом явился последующий выпуск очередного сервисного пакета Service Pack 4 для семейства NT 4.0, содержащего кроме средств адаптации к программно-аппаратной среде нового поколения и средства исправления очередной серии ошибок, выявленных в ходе эксплуатации этих операционных систем.

Тем не менее вскоре в компьютерной печати появились сообщения о выявлении серьезной ошибки в системе защиты Windows NT. В результате этой ошибки при определенных условиях пользователи DOS-клиентских рабочих станций могли получить неограниченный доступ к защищенным областям на серверах Windows NT.

В настоящее время в информационных системах специального назначения нередко используют операционную систему Linux, принадлежащую к семейству UNIX. Основными достоинствами ее являются повышенные устойчивость и производительность, характерные для UNIX-систем, и самое главное – бесплатность. Однако бесплатность этой системы основывается на открытости и общедоступности исходного кода ее ядра. Поэтому данный вопрос требует тщательной проработки, особенно в части, касающейся системы защиты данной операционной системы.

Безусловно, в документах, регламентирующих работу каналов передачи данных, предусмотрены специальные режимы обработки закрытой информации на средствах вычислительной техники. Однако это не позволяет полностью исключить угрозу нарушения работоспособности каналов передачи данных в условиях интенсивного информационного противоборства. Тем не менее, по нашему мнению, необходим системный комплексный подход к преодолению проблем в этой области. Интеграция даже имеющихся способов позволяет существенно повысить эффективность защиты каналов передачи данных в условиях современного информационного противоборства (таблица 2).

Следовательно, в настоящее время безопасность каналов передачи данных информационных систем специального назначения [4] означает нечто большее, чем просто информационная безопасность, обусловленная применением разрозненных способов защиты. Необходима интеграция всех средств и методов защиты каналов передачи данных с целью получения синергетического эффекта в этой области. Поэтому актуальными остаются:

а) требования разработки принципиально нового подхода к организации защиты информации с использованием синергетического эффекта;

б) мероприятия по развитию концептуальных подходов к принципам, стратегии и практике защиты информации в условиях информационного противоборства.

В интересах формирования этих подходов, как следует из результатов анализа накопленного опыта, целесообразно использовать инфологическую модель защиты информации в каналах передачи данных. Основными взаимосвязанными элементами такой модели являются:

состояния существования информации;

защитные свойства информации;

меры по защите информации в условиях информационного противоборства.

Кроме того, следует обратить внимание на сложность задач, связанных с защитой информации в каналах передачи данных. Это обусловлено следующими концептуальными положениями, характерными для любой системы специального назначения:

а) информация в системах специального назначения существует, как правило, в состояниях: передачи, хранения и обработки;

б) в каждом из перечисленных состояний защите подлежат такие свойства информации, как: конфиденциальность, целостность и полезность;

в) реализацию мер защиты применительно к каждому из названных свойств, в свою очередь, целесообразно разделить на три категории: технология, стратегия и тактика, обучение и тренировки.

В результате получаем 27 трехмерных совокупностей, каждая из которых может рассматриваться независимо друг от друга. Причем в каждой из них могут разрабатываться собственные способы защиты каналов передачи данных.

Справедливость рассмотренных концептуальных положений подтверждается практикой. Например, на таких принципах построена концептуальная модель безопасности информационных систем Джона МакКамбера или INFOSEC-модель.

Из логики построения модели следует, что она носит интегративный характер. Действительно, такая модель может включать в себя не только директивные мероприятия, предусмотренные руководящими документами по защите информации или используемыми программными, или техническими средствами. Ценность такой модели состоит в том, что здесь возможно комплексное использование любых целесообразных способов защиты, непосредственно вытекающих из складывающейся в данный момент ситуации, возникающей в процессе информационного противоборства. Кроме того, важен и следующий вывод: для успешной борьбы с деструктивным вмешательством в работу защищаемых систем необходимы не только технические и программные средства, но и понимание психологии и мотивов поведения нарушителей, постоянное внимание персонала информационных систем всех уровней к вопросам безопасности, их непрерывное обучение и тренировки.

Таким образом, анализ использования способов защиты каналов передачи данных в условиях информационного противоборства показывает, что:

во-первых, защита каналов передачи данных информационных систем специального назначения при грамотном системном подходе к ее построению

способна противостоять угрозам несанкционированного проникновения в информационные сети;

во-вторых, средства и методы защиты информационных систем специального назначения от воздействия поражающих факторов перспективных видов информационного воздействия еще далеки от совершенства и нуждаются в дальнейшем развитии и совершенствовании;

в-третьих, для повышения эффективности защиты каналов передачи данных в условиях информационного противоборства необходимо использовать возможности синергетического эффекта от интеграции всех разнородных сил и средств защиты информации.

Литература

1. Концепция национальной безопасности Российской Федерации, в редакции Указа Президента Российской Федерации № 24 от 10 января 2000 г.

2. Климов, С. М. Методы и модели противодействия компьютерным атакам / С.М. Климов. – Люберцы.: КАТАЛИТ, 2008. – 316 с.

3. Логунов, А. Б. Региональная и национальная безопасность / А.Б. Логунов. – М.: 2009. – 432 с.

4. Стрельцов, А. А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов // Информационное общество. – 2001. – Вып. 4. – С. 10–16.