sozdaniya i primeneniya malykh kosmicheskikh apparatov i robototekhnicheskikh sredstv: trudy Vserossijskoj nauchno-prakticheskoj konferentsii. SPb., 2016. T. 2. S. 234–239.
5. *Nechaj A.A.* Modelirovanie sistemy upravleniya robototekhnicheskim kompleksom likvidatsii chrezvychajnykh situatsij na osnove mnogomernykh kopula-funktsij // Sovremennye problemy sozdaniya i ekspluatatsii vooruzheniya, voennoj i spetsial'noj tekhniki: sbornik statej III Vserossijskoj nauchno-prakticheskoj konferentsii. SPb., 2016. S. 287–292.
6. *Nechaj A.A., Borisov A.A., Borisova Yu.I.* Tochechnyj analiz dannykh distantsionnogo zondirovaniya Zemli sredstvami yazyka programmirovaniya Python // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 1. S. 49–55.
7. *Nechaj A.A., Kop'ev A.I.* Metod upravlyaemogo raspredeleniya resursov mezhdu yadrami protsessora // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 101–107.
8. *Nikiforov A.Yu.* Zabluzhdeniya i real'nost' v oblasti otsenki radiatsionnoj stojkosti elektronnoj komponentnoj bazy // Spetstekhnika i svyaz'. 2011. № 4. S. 63–67.
9. *Pichkhadze K.M., Khamidullina N.M., Zefirov I.V.* Raschet lokal'nykh pogloshchennykh doz s uchetom real'noj konfiguratsii kosmicheskogo apparata // Kosmicheskie issledovaniya. 2006. T. 44, № 2. S. 179–182.
10. *Polesskij S. i dr.* Obespechenie radiatsionnoj stojkosti apparatury kosmicheskikh apparatov pri proektirovanii // Komponenty i tekhnologii. 2010. № 9. S. 93–98.
11. *Svinarchuk A.A., Kalinichenko S.V., Nechaj A.A.* Ispol'zovanie graficheskogo protsessora dlya uskoreniya raspredelennykh vychislenij pri prognoze ekstremal'nykh znachenij temperatury vozdukha // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2017. Vyp. 4. S. 33–38.
12. *Svinarchuk A.A., Nechaj A.A.* Ispol'zovanie kvantovykh vychislenij pri vybore upravlencheskogo resheniya // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 31–36.
13. *Shajmardanov A.M., Nechaj A.A., Lepekhin S.V.* Matematicheskie modeli sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyatsiej // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 2. S. 27–39.
14. *Koebel F., Coldefy J.-F.* SCOC3: A Space Computer on a Chip an Example of Successful Development of a Highly Integrated Innovative ASIC: Microelectronics Presentation Days ESA/ESTEC. Noordwijk, 2010.
15. *Taylor B. et al.* Galileo GIOVE-A MEORAD Results and Analysis // IEEE Transactions on Nuclear Science. 2008. Vol. 55, № 6.

DOI: 10.25586/RNU.V9187.20.01.P.159 УДК 004.78.056

А.И. Гладышев, Г.Г. Буров

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассматриваются теоретические основы защиты информации и системы защиты телекоммуникационных систем, основные группы международных организаций стандартизации по защите информационных систем. Приведены примеры возможных целей, которые могут оказывать влияние на систему защиты.

Ключевые слова: угроза, проникновение.

A.I. Gladyshev, G.G. Burov

ORGANIZATION OF PROTECTION OF INFORMATION SYSTEMS

The theoretical foundations of information protection and the protection system of telecommunication systems, the main groups of international standardization organizations for the protection of information systems are considered. Examples of possible goals that may affect the protection system are given.
Keywords: threat, penetration.

Спрос на защиту телекоммуникационных систем постоянно растет. Операторы сетей и провайдеры услуг больше не отказываются от применения систем защиты (СЗ) не только из-за роста компьютерного мошенничества, но и в связи с требованиями государственных и международных законов, указывающих на необходимость применения соответствующих механизмов защиты.

Во многих существующих системах телекоммуникаций при подтверждении идентификации для получения услуг, а также для управления ими используется только персональный идентификационный номер (PIN) или пароль. Данная «слабая идентификация» крайне ненадежна, поскольку велика вероятность подслушивания или замены PIN либо пароля. Вместо этого целесообразнее использовать механизмы защиты, основанные на криптографических ключах и алгоритмах шифрования [5].

Идентификация пользователя не является единственным аспектом защиты сети. Детальный анализ угроз новым услугам информационных систем (ИС), таких как универсальная персональная связь (Universal Personal Telecommunication, UPT) и беспроводная подвижная связь (Cordless Terminal Mobility, CTM), свидетельствует о том, что существует большое количество угроз, которые необходимо принимать во внимание. В случаях когда задействованы операторы и провайдеры услуг различных сетей, необходимо быть уверенным в том, что никто из них не нарушит доступ к объекту другой системы. Следует предотвратить нелегальную регистрацию объекта, подслушивание или модификацию передаваемых данных. Все это подразумевает, в зависимости от оценки риска, такие меры защиты, как эквивалентная идентификация объекта, проверка сохранности данных, кодирование и др. [2].

Основные группы международных организаций стандартизации по защите ИС и решаемые ими задачи:

- ETSI STC NA (IN)/SEG (группа экспертов по системам защиты):
  - построение системы защиты IN;
  - построение системы защиты UPT (в составе NA7); исследования по защите CTM.
- ETSI STC NA6 (IN)/UCG (группа по разработке карты UPT):
  - интерфейс между картой IC и устройством DTMF для карт UPT;
  - интерфейс между картой IC и терминалом.
- ITU – T: Q.29:
  - защита сети;
  - защита доступа.

Системы защиты (рис. 1) (с соответствующими модификациями) успешно использовались во многих исследовательских проектах и проектах по стандартизации (напри-

мер, европейский проект «Технология сохранности механизмов в IBCN» в рамках программы RACE, стандарт ETSI для защиты UPT, а также исследования ITU – T по защите FPLMTS).

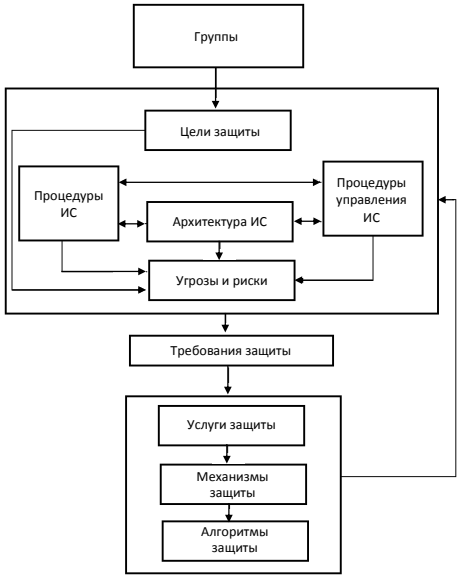

Рис. 1. Подход к построению системы защиты

Структурная схема (см. рис. 1) показывает логическую последовательность действий для построения системы защиты.

В качестве основы нужно иметь общий вид построения системы, характеристик и процессов, относящихся к системе защиты. Следует учитывать цели системы защиты всех задействованных групп [1].

На следующем этапе необходимо провести тщательный анализ всех угроз, включая оценку риска. Данный анализ угроз должен учитывать услуги ИС, задействованные группы и элементы системы, определенные в области системы защиты. На основе данного анализа угроз могут быть определены требования к системе защиты, а затем услуги, механизмы и алгоритмы.

Процедуру необходимо повторить во избежание неучтенных угроз. После учитываются общие цели системы защиты и общие условия угрозы и защиты [4].

Для ИС обсуждаются решения, принятые на основе существующей технологии по безопасной коммуникации и защите компьютера. Представляются конкретные решения для двух услуг ИС.

К услугам пользователей относятся аспекты, связанные с правильным функционированием и конфиденциальностью. Целью операторов сети и провайдеров услуг является получение хорошего годового дохода при работе в системе. У органов управления ИС существуют определенные требования, связанные с конфиденциальностью, хорошей защитой информации и инфраструктуры, ограничением использования криптографических методов и оправданностью действий [2].

Примеры возможных целей, которые могут оказывать влияние на СЗ:

- доступность и правильное функционирование процессов сети, услуг и функций управления;
- правильная и поддающаяся проверке оплата без возможности мошенничества;
- доступность для входящих звонков;
- возможность и правильное функционирование исходящих звонков;
- сохранность и конфиденциальность всей хранимой или передаваемой информации;
- возможность анонимного использования услуги;
- безотказная работа всех процессов сети и всех действий управления;
- защита репутации (сохранность доверия всех клиентов и инвесторов);
- учитываемость (ведение журналов) всех действий;
- ПО, удовлетворяющее общим критериям сертификации.

Цели, перечисленные выше, могут быть уменьшены до одной или до комбинации следующих основных целей, касающихся услуг ИС или управления ИС:

- конфиденциальность данных;
- сохранность данных;
- учитываемость;
- доступность.

Нелегальное проникновение в сеть (подлог) пользователя или системного элемента: объект может намеренно выступить в качестве другого объекта; это может послужить базой для возникновения других угроз, таких как несанкционированный доступ или подделка [6].

Несанкционированный доступ к элементам ИС: попытки объекта проникнуть в данные, что противоречит политике защиты.

Подслушивание на линиях связи: нарушение конфиденциальности, связанное с несанкционированным контролем сообщений.

Фальсификация информации: сохранность передаваемой информации подвергается опасности из-за несанкционированного удаления, вставки, модификации, переупорядочения, повторного проигрывания или задержки.

Отказ от подтверждения факта: объект, участвовавший в коммуникационном обмене, затем отказывается признать данный факт.

Подделывание: объект подделывает информацию и заявляет, что данная информация была получена от другого объекта или отправлена другому объекту.

Отказ от услуги: объект не в состоянии выполнить свою функцию или мешает другим объектам выполнить их функции.

Данные угрозы относятся к элементам ИС, а также к линиям связи. Потенциальные угрозы ИС показаны на рисунках 2–3.

На рисунке 2 SMP (узел администрирования услуг), например, может быть напрямую связан через LAN или ISDN с подписчиками, провайдерами услуг или веб-сервером. В связи с этим возникает угроза нелегального проникновения подписчика, провайдера услуг или веб-сервера, которые могут получить доступ к данным SMP несанкционированным способом. Передаваемая информация может быть подслушана или модифицирована.

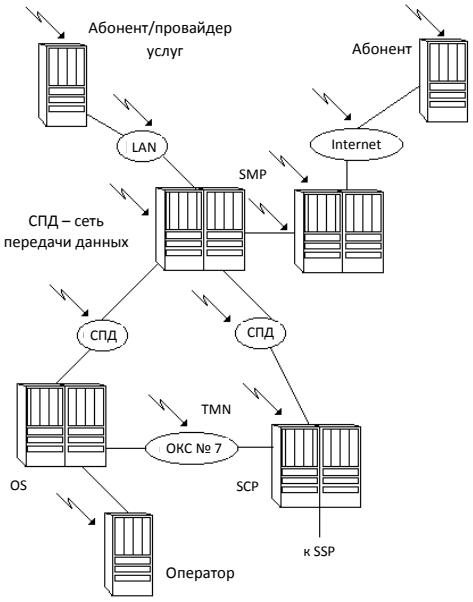

Рис. 2. Потенциальные угрозы ИС

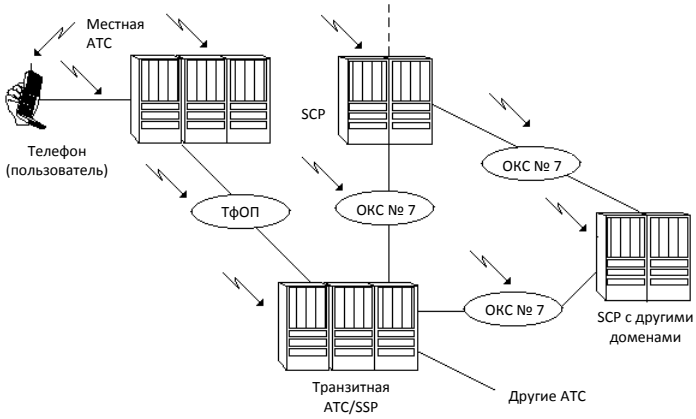

Рис. 3. Потенциальные угрозы для услуг использования ИС

Подписчик может связаться через Интернет с веб-сервером для контроля своих услуг ИС. Поэтому возникает угроза нелегального проникновения подписчика в Интернет или данные этого подписчика могут быть подслушаны либо модифицированы. Сеть управления (TMN) ИС включает управление конфигурациями, ошибками и рабочими характеристиками. Если во время передачи аварийный сигнал, являющийся частью данных управления ошибками, модифицируется, возникает возможность отказа от услуг ИС. Несанкционированный доступ к данным управления конфигурациями может привести к модификации конфигурации ИС для подключения враждебного SMP [3].

Во многих существующих ИС используется только PIN для определения подлинности подписчика услуг ИС. Данная «слабая идентификация» является крайне ненадежной, поскольку велика вероятность подслушивания или замены PIN [4].

Нелегальное проникновение SCP в SSP может иметь опасные последствия, такие как фальшивые звонки, неправильные счета на оплату или отказ в предоставлении услуг ИС.

Перед внедрением механизмов защиты против потенциальной угрозы данная угроза должна быть тщательно изучена. Всегда необходимо учитывать:

- какова вероятность угрозы (вероятность возникновения)?
- каков потенциальный ущерб (влияние)?
- какова стоимость предотвращения угрозы посредством СЗ?

Вероятность возникновения угрозы и ее влияние можно подразделить на три категории: 1 – низкая/низкое, 2 – средняя/среднее, 3 – высокая/высокое. Риск является следствием вероятности возникновения и влияния.

Только если риск представляется высоким, а потенциальный ущерб превышает стоимость адекватного решения СЗ против данной угрозы, данное решение будет приведено в действие.

Риск потенциальной угрозы сильно зависит от конкретной реализации ИС, от индивидуальной услуги ИС и от реализаций механизмов защиты (например, PIN или сложная идентификация, расположение идентификации, ключевое управление и т.д.).

На практике риск может возникнуть при частых попытках нарушения защиты сети и ее злоумышленного использования. Можно определить следующие угрозы, представляющие наиболее опасные варианты риска: нелегальное проникновение другого пользователя (особенно с точки зрения оплаты услуг!), подслушивание секретной информации (например, PIN), модификация данных пользователя.

Выбор механизмов защиты может зависеть от индивидуальной услуги ИС, ввода в работу системы ИС, физического окружения, в котором находятся элементы системы, а также от взаимного доверия и отношений между задействованными организациями. Общее решение должно быть принято в кратчайшие сроки [5].

На основе определенных целей, описанных угроз и вариантов риска функциональные требования к системе защиты представлены для тех элементов и соединений, потенциальный риск которых оценивается как наиболее высокий (рис. 4).

Подтверждение идентификации пользователя/подписчика (если возможно)
Подтверждение идентификации коммуникационного партнера
Гарантия конфиденциальности данных
Гарантия сохранности ПО и данных
Не отказ от действий
Определение попыток нарушения защиты

Рис. 4. Требования к системе защиты для элементов ИС

В таблице представлена зависимость между угрозами и функциональными требованиями к СЗ. Она составлена на основе результатов группы защиты ETSI TMN.

Угрозы и требования к системе защиты

Требование к системе защиты	Виды угроз						
	Угрозы элементам ИС					Угрозы во время передачи	
	Нелегальное проникновение	Несанкционированный доступ	Отказ подтверждения	Мошенничество	Отказ от выполнения услуги	Подслушивание	Фальсификация
Подтверждение идентификации	*	*	*	*	*		
Гарантия конфиденциальности ХД		*			*		
Гарантия сохранности ХД и ПО		*			*		
Неотказ от действий	*		*	*			
Определение попыток нарушения защиты	*	*	*	*	*	*	*
Гарантия сохранности КД						*	
Гарантия конфиденциальности КД							*

Примечание. ХД – хранимые данные; КД – коммуникационные данные.

Каждое требование к СЗ должно быть выполнено посредством одной услуги защиты (см. рис. 5).

Идентификация пользователя для провайдеров услуг и подписчиков
Экспертная идентификация коммуникационного партнера
Контроль доступа к ПО и данным
Безотказность
Запись действий
Регистрация аварийных сигналов СЗ
Периодическая проверка СЗ

Рис. 5. Услуги защиты для элементов ИС

Каждая услуга осуществляется за счет одного из механизмов СЗ. Например, механизмы экспертной идентификации объекта могут быть основаны на замене защищенного пароля, секретного ключа, общедоступного ключа или хешированных технологий. Механизм индивидуальной идентификации применим к односторонней и взаимной идентификации. Односторонняя идентификация означает, что только одна из двух взаимодействующих сторон (вызывающая сторона) идентифицирована для другой стороны (при-имающей стороны). При взаимной идентификации обе стороны идентифицируют друг друга.

Каждый механизм СЗ может использовать определенный алгоритм. Например, механизм идентификации, основанный на секретных ключах, может использовать один из следующих алгоритмов: DES, тройной DES или алгоритм FEAL и т.д.

Могут быть полезными чисто организационные меры, например управление качеством, контролируемый вход в помещение, ответственность сторон, оговоренная в контракте. Если риск продолжает представлять большую опасность, количество услуг должно быть уменьшено, а платежи ограничены определенными суммами [5].

Решения СЗ (рис. 6) основываются на следующих предположениях:

- SMP, SCP и OS (Operation System) вводятся в действие на стандартной платформе UNIX с элементами защиты UNIX.
- На используемых линиях передачи (через LAN, ISDN, Интернет) не были реализованы услуги конфиденциальности и сохранности информации.

Для обеспечения безопасной связи между подписчиками/провайдерами услуг и SMP можно использовать существующие криптоблоки.

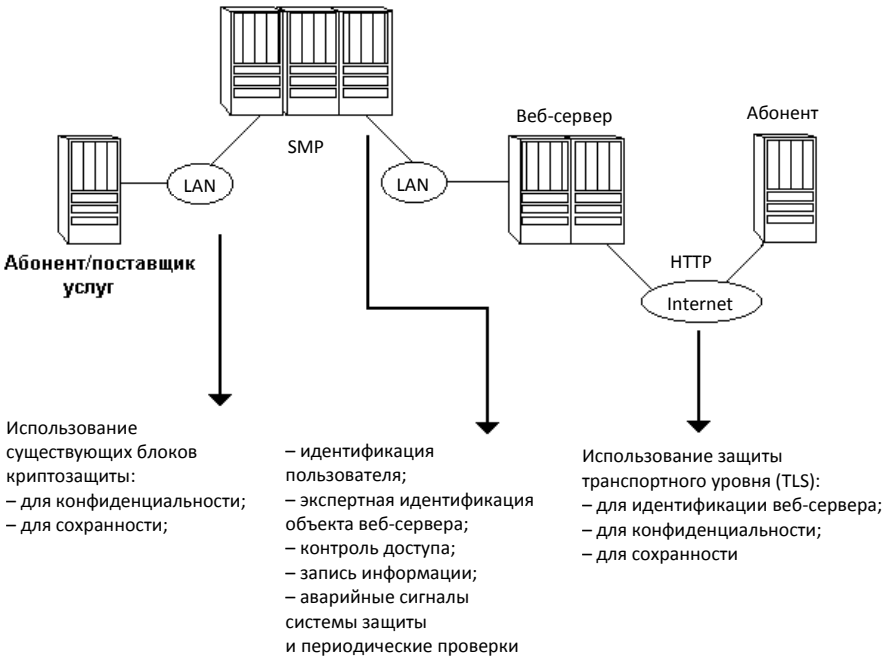

Рис. 6. Решения системы защиты для управления ИС

Для идентификации пользователя допустимо заменить защищенные пароли или смарт-карты с проверкой местного PIN.

Эквивалентная идентификация объекта веб-сервера может быть осуществлена использованием повторяемых защищенных паролей, секретных ключей, общедоступных ключей или механизмами, основанными на хеш-технологиях.

Передачу информации в сетях общего пользования возможно обезопасить, используя защиту транспортного уровня (TLS).

В заключение можно сказать, что концепция ИС принята и с успехом реализуется многими операторами и администрациями связи в развитых странах. Существующие решения, пусть даже не в полной мере соответствующие международным стандартам и рекомендациям, уже приносят немалые доходы.

Литература

1. *Вагнер Г.* Основы исследования операций. М.: Мир, 1972. 349 с.
2. *Гладышев А.И., Жуков А.О.* Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. 2013. Вып. 4. С. 53–55.
3. *Ефимов В.В.* Нейроподобные сети в бортовых информационно-управляющих комплексах летательных аппаратов. СПб.: ВИККА им. А.Ф. Можайского, 1996. 113 с.
4. *Корбут А.А., Финкельштейн Ю.Ю.* Дискретное программирование. М.: Наука, 1969. 318 с.
5. *Назаров А.В., Лоскутов А.И.* Нейросетевые алгоритмы прогнозирования и оптимизации систем. СПб.: Наука и техника, 2003. 384 с.
6. *Осовский С.* Нейронные сети для обработки информации / пер. с пол. М.: Финансы и статистика, 2002. 344 с.

Literatura

1. *Vagner G.* Osnovy issledovaniya operatsij. M.: Mir, 1972. 349 s.
2. *Gladyshev A.I., Zhukov A.O.* Dostoinstva i nedostatki imitatsionnogo modelirovaniya s ispol'zovaniem nejronnykh setej // Vestnik Rossijskogo novogo universiteta. 2013. Vyp. 4. S. 53–55.
3. *Efimov V.V.* Nejropodobnye seti v bortovykh informatsionno-upravlyayushchikh kompleksakh letatel'nykh apparatov. SPb.: VIKKA im. A.F. Mozhajskogo, 1996. 113 s.
4. *Korbut A.A., Finkel'shtejn Yu.Yu.* Diskretnoe programmirovanie. M.: Nauka, 1969. 318 s.
5. *Nazarov A.V., Loskutov A.I.* Nejrosetevye algoritmy prognozirovaniya i optimizatsii sistem. SPb.: Nauka i tekhnika, 2003. 384 s.
6. *Osovskij S.* Nejronnye seti dlya obrabotki informatsii / per. s pol. M.: Finansy i statistika, 2002. 344 s.