- **Plan (Планирование)** – фаза создания СУИБ, создание перечня активов, оценки рисков и выбора мер;
- **Do (Действие)** – этап реализации и внедрения соответствующих мер;
- **Check (Проверка)** – фаза оценки эффективности и производительности СМИБ. Обычно выполняется внутренними аудиторами.
- **Act (Улучшения)** – выполнение превентивных и корректирующих действий.

Литература

1. Стандарт ISO2700:2005
2. Материалы сайта BSI (http://www.bsi.ru)
3. Материалы сайта ISO (http://www.iso.org)

СОТОВЫЕ СЕТИ ГСМ И ИХ БЕЗОПАСНОСТЬ

Михал СЭРВА,
Политехнический институт (Вроцлав, Польша)

В Польше первые системы сотовых сетей стали доступными в 1991 году (фирма Центртел). Это была самая простая аналоговая сотовая сеть первого поколения 1Г (*first-generation*), работающая на частоте 450MHz. Она покрывала свыше 90% территории страны. Системы сотовых сетей подвергнуты угрозам безопасности в такой же степени, как и проводные сети. Кроме того, в отношении радиотрансфера информации появляются дополнительные опасности.

Аналоговые системы (первого поколения) не были защищены, прежде всего, от радиоперехвата и использования для создания клона телефона. Такой обман был довольно распространенным в данном типе сотовых сетей и стал причиной больших финансовых потерь операторов. Эти системы была также неустойчивы к перебоям. У них не было международного роуминга, а также передача данных происходила очень медленно. Это вызвало появление цифровой системы второго поколения 2Г (2G), называемой системой ГСМ. Теоретическая скорость данных в такой системе достигала 9,6 кб/с, а трансмиссия речи с кодированием колебалась в пределе 13 кб/с. Были добавлены также узкополосные услуги такие как: данные, SMS, VMS, Fax. Система ГСМ900 была в Польше внедрена в 1996 году фирмами: Польская Телефония Цифровая (PTC ERA GSM) и Полкомтел (PLUS GSM). Следующей системой была система 2,5Г (2,5G), к которой добавлена трансмиссия данных GPRS. Система 2,5Г стала переходной к технологии третьего поколения в которой добавлена трансмиссия EDGE. Это сделало возможным трансмиссию с теоретической пропускной

способностью 384 кб/с через инфраструктуру ГСМ, UMTS (imt-2000), а также стали развиваться интернетовские и мультимедийные функции. В 2011 году оператор П4 (PLAY) планирует внедрить новый стандарт 4Г. Система 4Г это только маркетинговое название, а не сеть четвёртого поколения, такая как в США, а только расширение уже существующей технологии UMTS. Ещё долгое время системы UMTS будут существовать вместе с технологией ГСМ.

Требования, предъявляемые к операторам сотовых сетей и касающихся безопасности, вызываны следующими обстоятельствами:

- всеобщий рост доступности телеинформационных услуг,
- открытость операционных систем,
- введение трансфера данных,
- соединение с сетями IP,
- рост преступной деятельности (вирусы, обманы, перехваты).

Источники опасности системы ГСМ (*Global System for Mobile Communications*).

Самыми распространенными источниками опасности являются такие, как мошенничество в сети путем перехвата секретных данных (также данных персональных абонентов), а также «перехват», то есть перехват разговора в реальном времени. Это было нетрудно сделать. Существует также возможность «подделаться» под абонента и выманивать системные услуги за счёт абонента.

Существуют три типа действий, которые должны обеспечить телеинформационную безопасность:

- аутентификация пользователя с идентификацией места, с которого происходит передача информации,
- проверка тождества потребителя с помощью цифровой подписи,
- конфиденциальность и доступность информации должна быть гарантирована только санкционированным потребителям.

В сегодняшних сотовых (цифровых) системах сфера безопасности дополняется криптографическими технологиями, например:

- цифровой подписью,
- кодированием данных,
- сообщениями трассировки.

Главной основой безопасности является полное отделение оборудования потребителя (например мобильный телефон, смартфон) от данных этого потребителя. Это стало возможно с помощью SIM-карты (*Subscriber Identity Module*). Самые важные данные, определяющие возможности доступа к услугам, записаны именно на SIM-карте. Такая SIM-карта идентифицирет абонента в сети ГСМ при помощи уникального номера (*IMSI - International Mobile Subsciber Identity*), который приписан только одному абоненту.

Угрозы безопасности сотовым сетям можно разделить на следующие группы:

- несанкционированный доступ,

- блокирование через процесс идентификации, используя электронную подпись,
- блокирование несанкционированного доступа через шифрование данных с помощью зашифрованного ключа,
- использование максимальной частности абонента через добавление TSMI (*Temporary Mobile Subscriber Identity*), то есть временный номер мобильного абонента, который делает возможным идентификацию настоящего абонента.

Исключение также использования несанкционированного (украденного) терминала, например мобильника, блокируя его IMEI (*International Mobile Equipment Identity*) у операторов сети.

Литература:

[1] Kabaciński W., Żal M.: *Sieci telekomunikacyjne,* WKŁ, Warszawa 12/2008.
[2] Simon A., Walczyk M.: *Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo*, Xylab, Kraków 2002.

ОРГАНИЗАЦИЯ СИСТЕМЫ ВНУТРЕННЕГО КОНТРОЛЯ

Лилия ПАВЛОВА,
IT&IS Management SRL (Республика Молдова)

Внутренний контроль затрагивает все сферы деятельности компании от целей бизнеса, включая эффективность и прибыльность, до сохранности ее ресурсов и защиты от мошенничества. Это контроль обоснованности принятия управленческих решений, которые могут оказать влияние на бизнес, а также принятие мер, предотвращающих мошенничество со стороны персонала.

Наиболее удачным и актуальным определением внутреннего контроля является определение в соответствии с моделью COSO (Committee of Sponsoring Organizations).

Внутренний контроль – это процесс, осуществляемый советом директоров, руководством и другим персоналом компании, который направлен на обеспечение разумной уверенности в том, что будут достигнуты цели организации в следующих аспектах:

- эффективность и результативность деятельности;
- достоверность финансовой отчетности;
- соответствие деятельности действующему законодательству.

При организации системы внутреннего контроля (СВК) необходимо руководствоваться следующими документами: