чтобы своевременно обеспечивать надлежащих людей надлежащей информацией [1]. Банковские ИС включают компьютеры, объединенные в сеть, и средства телекоммуникаций. ОО – это совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе эксплуатации ИС [1]. Названные методы и средства описываются в различных инструкциях, положениях, правилах и других организационных документах.

В докладе сравнивается ОО ИС «Банка 1» с аналогичным для другого белорусского банка средней величины (назовём его «Банк 2»). Цель сравнения – проверка того, насколько ОО ИС «Банка 1» является типичным для белорусских средних по величине банков. Особое внимание уделяется защите от потерь за счет отказов составных частей ИС.

Одинаковыми по названию и примерно одинаковыми по содержанию в обоих банках является «Политика информационной безопасности (ИБ) банка».

Практическая реализация основных положений перечисленных документов осуществлена в штатном расписании подразделений банков, ответственных за обслуживание, эксплуатацию и безопасность ИС, и в различных организационных документах.

В отличие от Банка1 штатное расписание Банка 2 включает:

управление безопасности в составе одного отдела (экономической безопасности) и двух секторов (сектора верификации и сектора розничного бизнеса).

департамент информационных технологий в составе двух управлений (управление развития информационных систем, управление эксплуатации информационных систем) и одного отдела (отдел информационной безопасности)

Численность специалистов в низовых подразделениях управлений (отдел и сектор) обоих соответствует пропорции 4:6:3:3:3:3 (в порядке упоминания подразделений).

Организационными документами Банка 2 в части информационной безопасности являются 3 положения («О категорировании информационных ресурсов», «Об оформлении и контроле исполнения прав доступа к программным и информационным ресурсам», «О применимости контролей»), 2 инструкции («Об организации парольной защиты», «По организации антивирусной защиты»), 2 правила («Работы с внешними устройствами», «Работы с мобильными компьютерами») и 1 порядок («Использования информационных ресурсов»). Сравнение показывает, что число вышеперечисленных организационных документов в Банке 2 превышает аналогичное для Банка 1, зато в Банке 1 имеется отсутствующая в Банке 2 «Концепция ИБ банка».

Таким образом, в Банке 2 главным документом в части потерь информации из-за отказов является локальный нормативный правовой акт «Политика Информационной Безопасности», в котором банк устанавливает общие требования по обеспечению информационной безопасности для следующих областей: а) назначение и распределение ролей и доверия к сотрудникам; б) стадии жизненного цикла автоматизированной банковской системы (АБС); в) защита от несанкционированного доступа, управления доступом и регистрацией в АБС; г) антивирусная защита; д) использование ресурсов Интернет; е) использование средств криптографической защиты информации; ж) защита банковских платежных и информационных технологических процессов; з) использование корпоративной электронной почты.

Назначенные приказами и распоряжениями Председателя Правления Банка лица (эксперты) при построении системы управления информационной безопасности должны действовать на основании Политики Информационной Безопасности и своих должностных инструкций, утверждаемых в установленном порядке.

Список использованных источников:

1. Шарлан А. И., Шеремет Д. В. Анализ состава организационного обеспечения информационных систем банка в части защиты информации // Тезисы докл. 48-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению

2. Информационные системы и технологии / под ред. В. Л. Николаенко и Г. В. Сечко, Минск: БГУИР, ИИТ, 7 – 11 мая 2012 года. – Мн.: ИИТ БГУИР, 2012. – 58 с. с ил. – С. 35.

ОПЫТ ПОДДЕРЖАНИЯ РАБОТОСПОСОБНОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ ОХРАНЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Матюшонок И. В., Вильчицкий А. Н.

Сечко Г. В. – канд. техн. наук, доцент

В современных системах охраны объектов одной из главных задач является обеспечение и повышение надежности оборудования. В докладе даются предложения по решению этой задачи исходя из опыта работы с системой интегрированной безопасности ИСБ «777»

В настоящий момент каждая организация, независимо от рода деятельности, применяет массу усилий и средств для обеспечения защиты своего имущества и пресечения несанкционированных попыток проникновения в контролируемую зону или несанкционированного выхода из зоны. Для этого необходимо создать все необходимые для защиты объекта: охранная и тревожная сигнализация; система охраны периметра; система контроля и управления доступом; система видеонаблюдения; пожарная сигнализация,

система оповещения. Для совместного выполнения функций всех подсистем и интегрирования их в одну систему возможно использовать интегрированную систему охраны (ИСО).

Для охраны объектов в СНГ наиболее широко используются интегрированные автоматизированные системы следующих видов:

для охраны промышленных предприятий, зданий учреждений и организаций, а также офисных зданий – интегрированная система безопасности (ИСБ) «777», ИСО «Орион», и др.;

для технического обеспечения бескараульной охраны складов вооружений и спецобъектов Министерства обороны и организации пресечения попыток проникновения на охраняемый военный объект – автоматизированная система охраны складов вооружений (АСОСВ) «СКАТ» и др.;

для технического обеспечения охраны объектов отбывания наказаний (тюрем) – автоматизированная система охраны тюрем (АСОТ) «АЛМАЗ» и др.;

и целый ряд других ИСО, отличающихся назначением, составом подсистем и уровнем интеграции (имеется в виду, что АСОСВ «СКАТ» и АСОТ «АЛМАЗ» включают в свой состав ИСБ «777»).

Каждая ИСО имеет оптимальный для своего назначения состав и структуру, обладает широкими программно-аппаратными возможностями. Система имеет модульное построение, гибкие программные настройки, минимальный состав оборудования. Это позволяет создать комплексы безопасности исходя из требований объектов с учетом их особенностей.

Модульный принцип построения исключает избыточность оборудования и обеспечивает при этом высокую функциональную возможность ИСО. Это позволяет сократить расходы на ее создание, снизить энергопотребление по сравнению с другими системами. Каждый модуль легко подвергается настраиванию на необходимый вариант применения. При применении ИСО нет необходимости в большом подменном фонде оборудования. Замена вышедших из строя модулей производится без дополнительных настроек.

Помимо отслеживания событий, в ИСО ведется непрерывный контроль и отображение состояния питания каждого модуля и качества связи с ним. Это существенно облегчает процесс пуско-наладки, снижает время и затраты на его проведение. Высокая информативность обеспечивается использованием разных способов индикации и отображения событий и состояний в системе – светодиодными индикаторами, текстами на экранах клавиатур и компьютера, активной графикой на экране монитора.

В докладе освещается практический опыт работы по поддержанию работоспособности технического и программного обеспечения ИСБ «777», установленной в исправительном учреждении Республики Беларусь. Даются конкретные предложения по повышению коэффициента готовности и других характеристик надёжности ИСБ. Для оценки одного из показателей информационной безопасности ИСБ как информационного объекта (ИО) предлагается использовать показатель потерь информации (ПИ) относительно отказов и сбоев. При этом под ИО понимается среда, в которой информация создается, передается, обрабатывается или хранится [1]. Согласно [2, 3] ПИ информационного объекта относительно отказов и сбоев в процентах может быть оценен как разность ста процентов и умноженного на 100 % коэффициента готовности ИО. В докладе оцениваются перспективы применения показателя потерь информации относительно отказов и сбоев для оценки информационной безопасности ИСБ «777» и ИСО в целом.

Список использованных источников:

1. Голиков В.Ф., Лыньков Л.М., Прудник А.М., Борботько Т.В. Правовые и организационно-технические методы защиты информации. – Мн.: БГУИР, 2004. – 81 с.

2. Гайдук В.Ю., Сахнович К.Е., Сечко Г.В., Федюкович А.М. Уровень защиты информации в компьютерах относительно одной из угроз техногенного характера // Материалы 14-й межд. НТК «Комплексная защита информации», 19-22 мая 2009 года, Могилёв / Российско-белорусский журнал «Управление защитой информации». – Мн.: НИИТЗИ, 2009. – С. 75.

3. Блинцов А.Е., Моженкова Е.В., Соловьянчик А.Н., Сечко Г.В., Турок А.С., Шеремет Д.В. Использование показателя потерь информации за счёт отказов для оценки степени информационной безопасности // Материалы 16-й межд. НТК «Комплексная защита информации», 17-20 мая 2011 года, Гродно. – Мн.: БелГИСС, 2011. – 345 с. – С. 174-176.

ПРОГРАММНОЕ СРЕДСТВО ОБРАБОТКИ НАВИГАЦИОННОЙ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мозолевская В. Н.

Моженкова Е. В. – м-р техн. наук, ассистент

Решается задача создания программного средства, которое позволит сократить время при внесении изменений в географическую карту и упростить процесс внесения изменений, так как полноценного аналога его, позволяющего добавлять векторные и точечные объекты в картографический материал на основе визуального материала и аудио меток, в настоящее время не существует

С исследованием космоса ученые стало возможно использовать сигналы спутника для навигации. Сегодня в составе GPS находится более 30 искусственных спутников Земли. Около 100 компаний производят 600 типов приемной аппаратуры, которая используется в самых различных отраслях человеческой деятельности: от авиации и транспорта до строительства и земледелия. В настоящее время, с помощью навигационной спутниковой системы получают информацию