ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Карпеко Е.Ю., 4 курс,
Белова С.В., ст.преподаватель,
УО «Белорусский национальный технический университет»

Для обеспечения информационной безопасности необходим комплексный системный подход. Для защиты информационной системы требуется сочетать меры следующих уровней:

1) Законодательные меры обеспечения информационной безопасности – это законы, постановления, указы, нормативные акты и стандарты. Этот уровень является важнейшим для обеспечения ИБ. На законодательном уровне различают две группы мер:

– меры, направленные на создание и поддержание в обществе негативного (в том числе и с применением наказаний) отношения к нарушениям ИБ (меры ограничительной направленности);

– направляющие и координирующие меры, способствующие повышению образованности общества в области ИБ, помогающие в разработке и распространении средств обеспечения ИБ (меры созидательной направленности).

2) Административные меры – это действия, предпринимаемые руководством предприятия или организации для обеспечения информационной безопасности.

Главная цель мер административного уровня – сформировать Политику ИБ и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Политика безопасности – это совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации от заданного множества угроз безопасности.

Политика безопасности определяет:

– какую информацию защищать и от кого;
– какой ущерб принесет предприятию потеря или раскрытие определенных данных;
– источники угроз, виды атак;
– какие средства использовать для защиты каждого вида информации и т.д.

3) Процедурные меры – это меры безопасности, ориентированные на людей. На процедурном уровне можно выделить следующие классы мер:

– управление персоналом;
– поддержание работоспособности;
– реагирование на нарушения режима безопасности;
– планирование восстановительных работ.

4) Физические средства защиты. Сюда относится экранирование помещений, проверка поставляемой аппаратуры, средства наружного наблюдения, охрана, замки, сейфы, перегородки, телекамеры, датчики движения и т.д. Основные направления физической защиты:

– физическое управление доступом;
– противопожарные меры;
– защита поддерживающей инфраструктуры;
– защита от перехвата данных;
– защита мобильных систем.

Для выбора оптимального средства целесообразно провести анализ рисков. Есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

5) Программно-технические – это меры, направленные на контроль компьютерных сущностей – оборудования, программ и данных, образуют последний и самый важный рубеж ИБ. Программно-технические меры реализуются программным и аппаратным обеспечением узлов и сети. Центральным для программно-технического уровня является понятие сервиса безопасности.

К основным сервисам (или функциям) безопасности относятся: идентификация и аутентификация; управление доступом; протоколирование и аудит; конфиденциальность; контроль целостности; экранирование; анализ защищенности; обеспечение отказоустойчивости; обеспечение безопасного восстановления; туннелирование; управление.

Программно-технические меры безопасности можно разделить на следующие виды:

– превентивные, препятствующие нарушениям ИБ;
– меры обнаружения нарушений;
– локализующие, сужающие зону воздействия нарушений;
– меры по выявлению нарушителя;
– меры восстановления режима безопасности.

Проверенная архитектура безопасности способна обеспечить управляемость ИС и способность противостоять все новым угрозам. Базовые принципы архитектурной безопасности:

– непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
– принцип единого контрольно-пропускного пункта;
– следование признанным стандартам, использование апробированных решений;
– усиление самого слабого звена;
– невозможность перехода в небезопасное состояние (использование средств, которые при отказе переходят в состояние максимальной защиты);

– минимизация привилегий;
– разделение обязанностей;
– эшелонированность обороны;
– разнообразие защитных средств или использование комплексного подхода к обеспечению безопасности;
– простота и управляемость ИС;
– минимизация объема защитных средств, выносимых на клиентские системы, так как конфигурацию клиентских систем трудно или невозможно контролировать;
– принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение.