РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

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

Пилипенко Д.А.

Кучинский П.В. – д-р ф-м. наук, профессор

Сегодня уже всем ясно, насколько важна защита информационных ресурсов. Многие также понимают, что система информационной безопасности — это не просто защита от прямых материальных потерь, но и конкурентные преимущества, репутация на рынке и более высокая степень доверия со стороны клиентов и партнеров. Поэтому на данный момент финансовые вложения в защиту своих ресурсов в том или ином объеме сделаны практически во всех компаниях: отдельные средства или комплексные системы безопасности установлены в каждой ИТ-системе.

Основная задача на этапе эксплуатации системы — это поддержание достигнутого уровня безопасности. Данное требование является таким же жестким, как и требование обеспечения отказоустойчивости ИТ-компонентов и непрерывности работы информационной системы в целом.

Современные угрозы безопасности в принципе преодолимы, уязвимости — устранимы, и в целом задача обеспечения защиты ресурсов выполнима. Именно поэтому так необходимо грамотно эксплуатировать и поддерживать систему безопасности предприятия. Это подразумевает проведение целого комплекса непрерывных и периодических работ, таких как техническая поддержка средств защиты, мониторинг и анализ событий безопасности, происходящих в системе, периодический контроль защищенности ресурсов, преодоление нештатных ситуаций и ликвидация последствий.

Для выполнения названных работ, во-первых, требуется соответствующее техническое и программное обеспечение, а во-вторых, нужен персонал необходимой численности, квалификации и имеющий достаточный опыт. Современные технологии безопасности действительно довольно эффективны, но они все равно не заменят человека, его мышление и опыт, особенно в преодолении критических проблем в системе защиты корпоративных ресурсов.

Система информационной безопасности предприятия была разработана на основе следующих принципов:

1) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

Тщательная идентификация активов позволяет выявить возможных нарушителей информационной безопасности, определить возможные методы проведения атак, идентифицировать угрозы и, следовательно, определить перечень задач, возлагаемых на систему информационной безопасности.

2) Законность. Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

Работы этапа системы безопасности проводятся и документируются в соответствии с требованиями ГОСТ 34.201-89 «Автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», ISO/IEC 17799:2000(E) «Информационные технологии. Правила управления информационной безопасностью».

3) Комплексное использование сил и средств. Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

Система информационной безопасности создается с учетом особенностей информационных систем и реализуется комплексом согласованных между собой организационных и технических мер, поддерживается соответствующими управленческими решениями. Для создания системы информационной безопасности, в первую очередь, разрабатываются процессы информационной безопасности и только во вторую очередь проектируются и внедряются программно-аппаратные комплексы системы безопасности, служащие для обеспечения процессов информационной безопасности.

4) Координация и взаимодействие внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия.

Отдельным компонентом обследования является сбор и анализ всей информации, непосредственным образом связанной с обеспечением информационной безопасности — процессами управления в организации, персоналом, методами и средствами обработки информации.

При проведении исследования допускается использовать различные методы сбора информации, например, интервью, опросные листы, анкетирование. При необходимости используются инструментальные средства — программно-аппаратные сканеры сетевой безопасности.

5) Сочетание гласности с конспирацией. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль — предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6) Компетентность. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

Специалисты, занимающиеся поддержкой и обслуживанием систем безопасности, должны иметь высокую квалификацию в области информационной безопасности и смежных областях информационных технологий, поскольку набор используемых в большинстве компаний средств защиты довольно широк, а механизмы их работы усложняются год от года. Уровень подготовки персонала, ответственного за корректную и - главное - эффективную работу систем защиты, всегда должен соответствовать таким условиям работы. То есть необходимо обеспечить сотрудникам возможность проходить специализированное обучение по всему набору средств и систем защиты. В больших и сложных информационных системах выполнение этого условия также требует серьезных затрат.

7) Экономическая целесообразность. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

8) Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.)и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

9) Системность. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

В зависимости от характера защищаемых активов информационных систем, система информационной безопасности может выполнять функции межсетевого экранирования, антивирусной защиты, обнаружения и предотвращения атак, контроля веб-трафика, защиты электронной почты, беспроводных соединений, информации в каналах связи, противодействия утечке конфиденциальной информации, контроля соответствия установленной политике информационной безопасности, стандарту.

Таким образом, был разработан комплекс мер по обеспечению информационной безопасности предприятия. Данные меры позволяют предприятию, эксплуатирующему защищенные информационные системы, владеть информацией о реальном уровне безопасности (или уязвимости) корпоративных ресурсов и контролировать их. Это означает, кроме прочего, выявлять и пресекать нарушения, контролировать действия персонала (как пользователей, так и администраторов), избегать негативных последствий для бизнеса. В конечном счете, все это является серьезным обоснованием инвестиций в корпоративную безопасность.

Список использованных источников:

1. Захарченко, В. И., Меркулов, Н.Н., Халикян, Н.В Экономическая безопасность бизнеса / В.И. Захарченко, Н.Н. Меркулов, Н.В. Халикян. – О.: Наука и техника, 2009. – 176 с.

2. Мак, В.И. Система безопасности предприятия / В.И. Мак // Best of security. – 2006. - №1

3. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / В.И. Ярочкин 3-е изд. - М.: Академический проект: Трикста, 2005. - 544 с

4. Бевалекс [Электронный ресурс]. – Режим доступа: http://www.bevalex.by/