как высокая сложность и, соответственно, стоимость работ по защите персональных данных, а также понимание установленных требований защиты. Исходя из существующих проблем в данной области, необходимо обеспечить, чтобы работы по защите персональных данных при их обработке в информационных системах были неотъемлемой частью работ по созданию самих информационных систем.

Список нормативной и научной литературы:

1. Закон Республики Молдова «О защите персональных данных» №17 от 15.02.2007.
2. Закон Республики Молдова «Об утверждении Положения о Национальном центре по защите персональных данных, структуры, предельной штатной численности и порядка финансирования» №182 от 10.07.2008.
3. www.itsec.ru.

Александр Жека, *«INTEXNAUCA" S.A.*

АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

The art of information security auditing is not only a measurement of the quality of technical means of protection, but also in evaluating the quality of their service and level of business process organization. Key indicators should describe the status of all properties of the object, because this is the only way to make the right conclusion about the state of information security in the organization.

Важнейший ресурс современного общества – информация – одновременно несет в себе и огромную угрозу для него, связанную с внутренней спецификой этого ресурса. Простота и большое число различных способов доступа и модификации информации, значительное количество квалифицированных специалистов, широкое использование в общественном производстве специальных технических средств позволяют злоумышленнику практически в любой момент и в любом месте осуществлять действия, представляющие угрозу информационной безопасности как в локальном, так и в глобальном масштабах.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с определенными критериями информационной безопасности.

Основная задача аудита – объективно оценить текущее состоя-

ние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса по увеличению эффективности и рентабельности экономической деятельности компании.

Результаты аудита позволяют построить оптимальную по эффективности и затратам систему защиты корпоративной информации, адекватную текущим задачам и целям бизнеса.

Неоходимость аудита безопасности для вашей компании

Важной составляющей развития современных предприятий является автоматизация бизнес-процессов с использованием средств вычислительной техники и телекоммуникаций.

Следствием этого является неуклонный рост объемов информации, которая подвергается обработке и накоплению в электронном виде.

Рост электронного документооборота предприятия увеличивает зависимость успеха деятельности от непрерывности функционирования информационной системы (ИС). Функциональность ИС необходимо рассматривать с точки зрения единого целого путем обеспечения сохранности корпоративной информации в процессе ее обработки и хранения на электронных носителях.

Привыкая к повседневному использованию информационных технологий, мы часто забываем о том, что надежность техники и главное – устройств хранения электронной информации конечна, в связи с чем существует вероятность отказа оборудования, приводящая к сбоям в доступе к электронной информации, а в худшем случае – к частичной или полной ее потере. Более того, мы совсем не заботимся о разработке и внедрении плана мероприятий по восстановлению работоспособности ИС после кризиса.

Отказ оборудования зачастую происходит именно в тот момент времени, когда это наносит наибольший ущерб. Известны случаи, когда простой информационной системы приводил к экономическим убыткам, многократно превышающим стоимость самой системы.

Рост информационной системы предприятия, являющийся неминуемой частью успешного развития бизнеса, влечет за собой ужесточение требований к непрерывности ее функционирования, а также к сохранности и обеспечению конфиденциальности корпоративной информации. ИС предприятия превращается из печатной машинки в инструмент ведения бизнеса, что, в свою очередь, втягивает предприятие во все большую зависимость от уязвимости, постоянно усложняющейся ИС.

Отсутствие плана мероприятий по восстановлению работоспособности ИС после кризиса является одним из критических аспектов уязвимости. В случае возникновения форс-мажорных обстоятельств можно арендовать новое помещение, закупить технику, подключить телекоммуникации, но нельзя восстановить работоспособность ИС, если утрачена информация и/или специализированные средства ее обработки.

Очень важно понимать и осознавать, что:

- обеспечение информационной безопасности – это непрерывный процесс, взаимоувязывающий правовые, организационные и программно-аппаратные меры защиты;
- в основе этого процесса лежит периодический анализ защищенности информационной системы в разрезе видов угроз и динамики их развития;
- информационная система в своем развитии должна подвергаться периодическим реорганизациям, отправной точкой каждой из которых служит анализ выявленных уязвимостей при проведении аудита информационной безопасности.

Аудит информационной безопасности включает следующие этапы работ:

- Комплексный анализ информационных систем компании и подсистемы информационной безопасности на правовом, методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков;
- Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима ИС компании;
- Организационно-технологический анализ ИС компании;
- Экспертиза решений и проектов;
- Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации;
- — Работы, поддерживающие практическую реализацию плана защиты;
- — Повышение квалификации и переподготовка специалистов.

Аудит информационной безопасности должен быть ориентирован как на специалистов в области IT-безопасности, так и на специалистов в области менеджмента. Такой подход устраняет существующее недопонимание специалистов в области информационной безопасности ТОР-менеджерами компании.

Литература:

1. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. *Аудит информационной безопасности*. – М.: Издательская группа «БДЦ-пресс», 2006.
2. Игнатьев В.А. И 266 *Информационная безопасность современного коммерческого предприятия: Монография*. – Старый Оскол: ООО «ТНТ», 2005.
3. www.infosecurity.ru
4. www.bezpeka.com