УДК 004.03

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Михайлов Д.В.

CONCEPTUAL MODEL OF INFORMATION SAFETY OF THE ENTERPRISE

Michaylov D.V.

Обосновывается необходимость обеспечения информационной безопасности предприятий. Предлагается концептуальная модель построения корпоративной системы защиты информации, которая учитывает влияние объективных внешних и внутренних факторов на состояние информационной безопасности предприятия. Показано, что информационная безопасность представляет собой комплекс мер по обеспечению безопасности информационных активов предприятия. Решение каких-либо отдельных вопросов не решит проблему информационной безопасности в целом, её можно обеспечить только в случае комплексного подхода.

Ключевые слова: *предприятие, информационная безопасность, риск, конфиденциальность данных.*

Постановка проблемы. Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков. Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности предприятий, все более усиливается.

Современные методы управления рисками позволяют решить ряд задач перспективного стратегического развития предприятия. Во-первых, количественно оценить текущий уровень информационной безопасности предприятия, что потребует выявления рисков на правовом, организационно-управлен-ческом, технологическом и техническом уровнях обеспечения защиты информации. Во-вторых, в систему риск-менеджмента на предприятии может быть включена политика безопасности и планы совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании.

Анализ последних исследований и публикаций. Проблемы информационной безопасности предприятий постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Об актуальности проблемы свидетельствует её обширный анализ в многочисленных литературных источниках [1-10].

Беспрецедентные темпы развития и распространения информационных технологий, обострение конкурентной борьбы требуют создания целостной системы безопасности информации, взаимоувязывающей правовые, оперативные, технологические, организационные, технические и физические меры защиты информации, основываясь на научно-технических принципах построения систем обеспечения безопасности информационных ресурсов корпоративных сетей с учетом современных тенденций развития сетевых информационных технологий, а так же с использованием исследований по защите от внутренних нарушителей.

Цель. Целью работы является совершенствование концептуальной модели информационной безопасности предприятия, введением таких элементов, которые определяли бы эффективный и достаточный набор требований безопасности.

Результаты исследований. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач: конфиденциальность данных, которая

обеспечивается применением различных криптографических методов и средств; идентификация пользователя на основе анализа кодов, используемых им для подтверждения своих прав на доступ в систему (сеть), на работу с данными и на их изменение (обеспечивается введением соответствующих паролей, анализом электронной подписи). Перечень аналогичных задач, решаемых для обеспечения информационной безопасности и защиты информации в современных системах обработки и передачи данных, может быть продолжен. Интенсивное развитие современных информационных технологий, и в особенности сетевых технологий, для этого создает все предпосылки.

Бурный рост Internet вместе с существенным набором новых возможностей и услуг приносит и ряд новых проблем, наиболее неприятной из которых, безусловно является проблема безопасности. Даже беглый анализ компьютерной прессы показывает, что проблема безопасности и сохранности информации, помещаемой в Internet или во внутренние корпоративные Intranet-системы, стоит достаточно остро. Поэтому неудивительно, что все компании-производители программного обеспечения для Internet вводят в свои продукты все более совершенные средства защиты информации. Internet и информационная безопасность несовместимы по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров. Серьезный сбой локальных сетей может парализовать работу предприятия, что приводит к ощутимым материальным потерям.

Основными объектами информационной безопасности на предприятии являются: информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления; процессы обработки информации в автоматизированных системах, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков и пользователей системы и ее обслуживающий персонал; информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты автоматизированной системы.

Практика функционирования автоматизированных информационных систем показывает, что достижение 100 %-го уровня безопасности дело дорогое и не всегда целесообразное, так как даже самая совершенная на сегодня система информационной защиты не может противодействовать угрозам, которые могут возникнуть в последующем, а стоимость комплексной защиты может оказаться значительно выше, чем стоимость защищаемых информационных ресурсов.

Большую помощь в построении эффективной системы информационной безопасности могут оказать методы математического моделирования, с помощью которых можно выбрать оптимальный комплекс средств защиты, а также смоделировать, насколько созданная система информационной безопасности окажется эффективной в борьбе против наиболее распространенных угроз.

Безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе. Критериями информационной безопасности являются конфиденциальность, целостность и будущая доступность информации. При этом под конфиденциальностью понимается свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц. Целостность – это свойство информационных ресурсов, в том числе информации, определяющее их точность и полноту. В свою очередь доступность информации – это свойство, определяющее возможность получения и использования информации по требованию уполномоченных лиц.

Информационная безопасность представляет собой комплекс мер по обеспечению безопасности информационных активов предприятия. Решение каких-либо отдельных вопросов (технических или организационных) не решит проблему информационной безопасности в целом, её можно обеспечить только в случае комплексного подхода. Он ориентирован на создание защищенной среды обработки информации в корпоративной системе, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально-этические, организационные, программные и технические способы обеспечения информационной безопасности. Однако только

математическое моделирование корпоративной сети позволяет обеспечить эффективность и гарантированность функционирования систем защиты. Принцип построения системы безопасности информационных ресурсов корпоративной сети должен быть основан на научных предпосылках, научно-обоснованной математической модели, раскрывающей внутренние принципы функционирования организации. На основе математического моделирования можно будет построить обоснованную, с гарантиями по безопасности концепцию информационной безопасности организации.

Концепция является методологической основой для формирования и проведения в организации единой политики в области обеспечения безопасности информации (политики безопасности), для принятия управленческих решений и разработки практических мер по ее воплощению.

Все сотрудники предприятия, на каком бы уровне они ни работали, должны обучаться приемам защиты информации и всячески сотрудничать с ответственными за информационную безопасность. Необходимо, чтобы все, кто занимается обеспечением информационной безопасности, в каком бы подразделении они ни работали, помогали друг другу. Надо также, чтобы конечные пользователи поддерживали усилия по защите информации, понимали важность таких усилий и строго соблюдали все предписанные правила. Процесс постоянного обучения сотрудников должен быть подстроен под запросы конкретных групп и отделов. Внедрение системы информационной безопасности, как правило, приводит к более продуктивному использованию рабочего времени сотрудниками. Это связано, например, с ограничением доступа к информации, не требующейся для работы, в результате исключается доступ к развлекательным сайтам, а также уменьшается объем неслужебной переписки.

Система информационной безопасности должна базироваться на следующих принципах:

- прогнозирование и своевременное выявление угроз безопасности информационных ресурсов, причин и условий, способствующих нанесению финансового и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц и, тем самым, ослабление возможного негативного влияния последствий нарушения информационной безопасности.

При разработке модели информационной безопасности предприятия необходимо использовать международные нормативные документы ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», ISO/IEC 17799 «Управление информационной безопасностью».

Для эффективного функционирования системы информационной безопасности предприятия её необходимо оснастить комплексом аппаратных и программных средств защиты от различных информационных угроз.

При построении системы информационной безопасности предприятия предлагается модель (рис. 1), которая описывает совокупность объективных внешних и внутренних факторов и демонстрирует их влияние на состояние информационной безопасности на объекте. Данная модель включает следующие объективные факторы: угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации; уязвимости информационной системы или системы контрмер, влияющие на вероятность реализации угрозы; риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности – утечки информации и ее неправомерного использования.

Необходимо составить как можно более подробную карту информационной системы предприятия, т.е. описать, где и какое находится сетевое оборудование, какая ПЭВМ к какому порту подключена, и какие функции на ней выполняются, определить круг лиц, которым можно работать за конкретными ПЭВМ и их функциональные обязанности. Описать маршрут движения и права доступа к электронным документам. Проанализировать полученную информацию и разработать математические алгоритмы обеспечения информационной безопасности организации, соответствующие основополагающим целям защиты информационных ресурсов: доступность, целостность, секретность. В ходе анализа можно установить: какая угроза существует и ее тип, объект угрозы, от кого может исходить и каким методом можно устранить. При этом появляется динамическая модель взаимосвязей объектов в системе с управлением доступа на основе атрибутов.

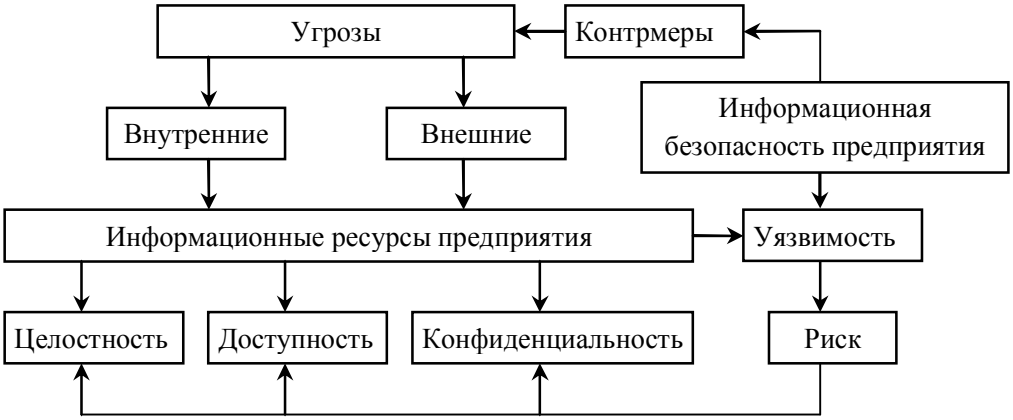

Рис. 1. Концептуальная модель информационной безопасности предприятия

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходы на дополнительные меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

Вывод. Таким образом, благодаря многоступенчатой структуре концептуальной модели информационной безопасности предприятия, введения системы контроля и закрепления ответственности, существенно снижается риск утечек конфиденциальной информации по вине человеческого фактора.

Литература

1. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: БХВ-Петербург; 2003. – 752 с.
2. Садердинов А.А. Информационная безопасность предприятия / А.А. Садердинов, А.А. Федулов, В.А. Трайнев. – М.: Дашков и Ко, 2004. – 336 с.
3. Петраков А. Информационная безопасность и защита информации / А. Петраков, В. Мельников, С. Клейменов С. – М.: Academia, 2008. – 336 с.
4. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия-Телеком, 2000. – 452 с.
5. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.
6. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО ТИД «ДС», 2004. – 992 с.
7. Степанов Е. Защита информации в офисе / Е. Степанов, И. Корнеев. – М.: ТК Велби, 2007. – 336 с.
8. Шелупанов А.А. Системный анализ в защите информации / А.А. Шелупанов, А.А. Шумский. – М.: Гелиос АРВ, 2005. – 224 с.
9. Козачок В. Основы организационного обеспечения информационной безопасности объектов информатизации / В. Козачок, С. Гребенев, С. Семкин, Э. Беляков. – М.: Гелиос АРВ, 2005. – 192 с.
10. Партыка Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2007. – 368 с.

References

1. Koneev I.R. Informacionnaja bezopasnost' predprijatija / I.R. Koneev, A.B. Beljaev. – SPb.: BHV-Peterburg; 2003. – 752 s.
2. Saderdinov A.A. Informacionnaja bezopasnost' predprijatija / A.A. Saderdinov, A.A. Fedulov, V.A. Trajnev. – M.: Dashkov i Ko, 2004. – 336 s.
3. Petrakov A. Informacionnaja bezopasnost' i zashhita informacii / A. Petrakov, V. Mel'nikov, S. Klejmenov S. – M.: Academia, 2008. – 336 s.
4. Zegzhda D.P. Osnovy bezopasnosti informacionnyh sistem / D.P. Zegzhda, A.M. Ivashko. – M.: Gorjachaja linija-Telekom, 2000. – 452 s.
5. Petrenko S.A. Upravlenie informacionnymi riskami. Jekonomicheski opravdannaja bezopasnost' / S.A. Petrenko, C.B. Simonov. – M.: Kompanija AjTi, DMK Press, 2004. – 384 s.
6. Domarev V.V. Bezopasnost' informacionnyh tehnologij. Sistemnyj podhod / V.V. Domarev. – K.: OOO TID «DS», 2004. – 992 s.
7. Stepanov E. Zashhita informacii v ofise / E. Stepanov, I. Korneev. – M.: TK Velbi, 2007. – 336 s.
8. Shelupanov A.A. Sistemnyj analiz v zashhite informacii / A.A. Shelupanov, A.A. Shumskij. – M.: Gelios ARV, 2005. – 224 s.
9. Kozachok V. Osnovy organizacionnogo obespechenija informacionnoj bezopasnosti obektov informatizacii / V. Kozachok, S. Grebenev, S. Semkin, Je. Beljakov. – M.: Gelios ARV, 2005. – 192 s.
10. Partyka T.L. Informacionnaja bezopasnost' / T.L. Partyka, I.I. Popov. – M.: Forum, 2007. – 368 s.

Михайлов Д.В. Концептуальна модель інформаційної безпеки підприємства

Обґрунтовується необхідність забезпечення інформаційної безпеки підприємств. Пропонується концептуальна модель побудови корпоративної системи захисту інформації, яка враховує вплив об'єктивних зовнішніх і внутрішніх чинників на стан інформаційної безпеки підприємства. Показано, що інформаційна безпека являє собою комплекс заходів щодо забезпечення безпеки інформаційних активів підприємства. Рішення будь-яких окремих питань не вирішить проблему інформаційної безпеки в цілому, її можна забезпечити лише в разі комплексного підходу.

Ключові слова: *підприємство, інформаційна безпека, ризик, конфіденційність даних.*

Michaylov D.V. Conceptual model of information safety of the enterprise

Necessity of provision of corporate information security. The conceptual model is proposed construction of a corporate information security system, which takes into account influence of objective external and internal factors on the state of security companies. It is shown that information security is a complex of measures to ensure the security of information assets. The solution of any issues not solve the problem of information security in General, it can be ensured only in case of complex approach. Thanks to a multi-structure of the conceptual model of information safety of the enterprise, introduction of system of control and allocation of responsibility, significantly reduced the risk of leaks of confidential information through the fault of the human factor. The concept is a methodological basis for the formation and organization of a unified policy in the field of information security (security policy) for management decisions and the development of practical measures for its implementation.

Keywords: *enterprise, information security, risk, confidentiality of data.*

Михайлов Д.В. – к.т.н., доцент кафедри охорони праці та БЖД, СНУ ім. В. Даля, м. Луганськ, Україна, e-mail: dm2007@land.ru.

Рецензент: **Погорелов О.О.,** д.т.н., проф.

Стаття подана 25.04.2013