

информация надежно защищена и система управления этой защиты работающая и адекватная современным условиям глобализации, рыночной конкуренции, мощному развитию информационных технологий, действию финансового и экономического кризиса. 4) Предприятие понимает и объективно применяет законодательство страны в области управления информационной надежностью, стандартов обеспечения непрерывности бизнеса при возникновении чрезвычайных ситуаций и кризисов и для управления риском. 5) Гарантируется конфиденциальность и интегритет информационных активов при помощи управления доступа к ним с применением необходимых и достаточных ресурсов для их защиты. 6) Повышается международное признание и авторитет предприятия как на внутреннем, так и на международных рынках.

ИНВЕНТАРИЗАЦИЯ РЕСУРСОВ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Анна МИЛОВАНОВА,

Швеция, Стокгольм, Lärcentrum

На сегодняшний день как крупные, так и небольшие организации характеризуются отсутствием четко определенной структуры имеющихся ресурсов, особенно с точки зрения критериев информационной безопасности.

В соответствии с национальным законодательством в автоматизированных системах защищается только информация ограниченного доступа и состояние информационной безопасности определяется критериями конфиденциальности, целостности и доступности ресурсов. Инвентаризация ресурсов в свою очередь позволяет решить ряд важных задач для построения эффективной системы обеспечения информационной безопасности, что доказывает необходимость ее проведения. Также она является одним из главных аспектов в управлении рисками внутренней информационной безопасности.

Важно отметить, что основной целью проведения инвентаризации ресурсов является обеспечение их соответствующей защитой. Проведение инвентаризации ресурсов обеспечивает достижение и следующих целей:

- ведение учета ресурсов и обеспечение уверенности в их защищенности;
- идентификация владельцев и собственников ресурсов, и определение их ответственности;
- идентификация относительной ценности ресурсов для управления рисками организации.

Приступая к инвентаризации ресурсов, необходимо внести определенность и четкость в используемые понятия, то есть обеспечить однозначность представления

используемых понятий руководством организации и различными структурными единицами. Так, ресурс подразумевает совокупность материальных благ принадлежащих одной организации (например, информационные, технические, программные и другие ресурсы, входящие в состав информационных систем).

При проведении инвентаризации необходимо определить критерии выделения категорий ресурсов, подготовить основу для постоянного ведения реестра ресурсов и создать нормативную базу разграничения доступа к ним. Согласно международным стандартам и практикам, среди которых ISO 17799 «Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасности», выделяют следующие категории ресурсов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, исследовательская документация, руководства пользователей, обучающий материал, рабочие процедуры, планы обеспечения непрерывности бизнеса и т.д.);
- программные ресурсы (прикладное, системное, инструментальное программное обеспечение и утилиты);
- физические ресурсы (компьютерное оборудование, оборудование связи, сменные носители и другое оборудование);
- сервисы (вычислительные службы и службы связи, службы общего назначения).

Классификация ресурсов не должна быть слишком сложной во избежание обременительности и неэкономичности, но при этом необходимо учесть все бизнес требования и внутренние требования организации.

Действия, выполняемые в ходе инвентаризации ресурсов, включают следующее:

- определение области проведения инвентаризации, то есть какие будут рассмотрены осуществляемые бизнес-процессы и выполняемые задачи;
- определение и классификация ресурсов (для информационных ресурсов также определение видов информации, таких как входящая, исходящая, хранимая, обрабатываемая информация);
- определение владельцев и собственников ресурсов;
- категорирование ресурсов по критериям информационной безопасности (например, общая информация, информация ограниченного пользования, государственная или коммерческая тайна и тд). Это позволяет выделить наиболее критичные ресурсы, нарушение информационной безопасности которых может привести к ущербу;
- определение субъектов ресурсов, то есть пользователей, которым предоставляется доступ к защищаемой информации (разграничение доступа и полномочий);
- регламентирование способов хранения и защиты критичных ресурсов, а также безопасной работы с ними в случае чрезвычайных ситуаций;
- документирование процесса инвентаризации ресурсов, включая инвентаризационные описи.

Необходимо отметить, что для обеспечения должного управления ресурсами следует руководствоваться следующим:

- ресурсы четко идентифицируются с учетом их относительной ценности и важности, а также с точки зрения критериев информационной безопасности;
- любой ресурс рассматривается с точки зрения технологии создания, обработки, хранения, отправки или приема информации;
- любой ресурс рассматривается с точки зрения разделения его на составные части;
- ресурсы учитываются и закрепляются за ответственными владельцами и/или собственниками;
- определяется ответственность за поддержание соответствующих мероприятий по управлению информационной безопасности, в случае делегирования обязанностей ответственность остается за назначенным владельцем ресурса;
- указывается фактическое местоположение ресурса, так как это является важным моментом при восстановлении ресурсов в случае их потери или повреждения.

Основываясь на полученной информации в результате инвентаризации ресурсов, организация может определить, какая информация должна быть обработана и защищена, то есть обеспечить заданные уровни защиты используемых информационных ресурсов. Это обусловлено тем, что некоторые виды информационных ресурсов могут потребовать дополнительной защиты или специального обращения.

Полученные результаты инвентаризации ресурсов в обязательном порядке должны быть оформлены в инвентаризационных описях по каждой категории ресурсов. После оформления инвентаризационных описей по каждой категории ресурсов составляется единый акт о проведении инвентаризации.

Так например, в инвентаризационных описях для информационных ресурсов рекомендуется отражать следующие параметры:

- вид ресурса (например, база данных, папка или файл);
- наименование ресурса;
- краткое содержание ресурса;
- принадлежность к функциональным подсистемам и прикладным сервисам;
- характер и вид информации;
- место размещения (например, имя компьютера, сервера, диска);
- список пользователей, имеющих доступ к ресурсу;
- размер ресурса;
- необходимый уровень защиты;
- необходимость резервного копирования.

Информационные ресурсы являются базовыми составляющими в части обеспечения управления и информационно-аналитической поддержки функционирования

организации вне зависимости от сферы деятельности. Исходя из этого, общие положения по инвентаризации ресурсов, порядок ведения учета ресурсов, правила формирования реестра информационных ресурсов, порядок сбора, анализа, пересмотра и контроля учетной информации об информационных ресурсах должны определяться внутренней организационно-распорядительной документацией организации.

Таким образом, инвентаризация ресурсов определяет важные сведения, необходимые для обеспечения информационной безопасности автоматизированных информационных систем. А как известно, построение эффективной системы информационной безопасности является одним из наиболее важных условий успешного функционирования любой ИТ-инфраструктуры, что в свою очередь становится критическим фактором успешного ведения бизнеса.

Литература:

1. ISO/IEC 17799:2005 «Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасностью»;
2. www.iso27000.ru;
3. www.itsec.ru.

ОСОБЕННОСТИ ТРАНСФЕРА РЕЗУЛЬТАТОВ НАУЧНО-ТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ВУЗА, СОДЕРЖАЩИХ ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

О. ПУГАЧЕВА,

Гомельский госуниверситет им. Ф. Скорины (Республика Беларусь)

In article features of a transfer of results of scientific and technical activity of the high school, containing objects of intellectual property are considered, and also the general algorithm of protection of not opened information is resulted

Вузовский сектор Республики Беларусь, обладающий значительным научно-техническим и инновационным потенциалом, играет важную роль в создании экономики инновационного типа. Практика показывает, что новая модель университета как учебно-научно-инновационного комплекса, сочетающего академическую науку с развитой сетью высокотехнологичных инновационных структур и малых предприятий, является одним из наиболее эффективных базовых элементов национальной инновационной системы.

Развитию инновационной деятельности в регионе способствует создание в Гомельском госуниверситете им. Ф.Скорины опытно-промышленных производств абразивного инструмента и полирующих суспензий для полировки пластин полупроводниковых и других материалов, договора на производство и поставку которых