УДК 338.246.87

ХРАНЕНИЕ И ЗАЩИТА ИНФОРМАЦИИ

Хачатурова С.С.

ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Москва, e-mail: seda_@mail.ru

В данной статье рассматривается актуальный вопрос хранения и защиты информации, который представляет актуальность для владельцев организаций, компаний, менеджеров отдельных подразделений. Так как информация в настоящее время представляет важнейшую ценность, то обеспечение ее безопасности, защита информации является одним из основных вопросов на пути к достижению успеха в бизнесе.

Ключевые слова: защита, безопасность, информация, хранения, создание, организация, бизнес, дело, виды, ресурс, проблема, конфиденциальность, сохранность, носители, сбой, повреждение

STORAGE AND DATA PROTECTION

Khachaturova S.S.

Plekhanov Russian of Economics, Moscow, e-mail: seda_@mail.ru

This article discusses the topical issue of storage and protection of information that is relevant for owners of organizations, companies, managers of individual units. Since information is now the critical value, then the security protection of information is one of the main issues on the path to success in business.

Keywords: protection, security, information storage, creation, organization, business, cause, species, resource, problem, privacy, security, media, crashing, damage

Информация – это ресурс, правильное использование которого может как принести успех фирме, так и помешать ее нормальному развитию. В связи с этим важной задачей любой организации, будь то некрупная фирма или большая корпорация, является хранение и защита информации. В настоящее время количество информационного ресурса непрерывно увеличивается. Типов, видов информации стало настолько много, что бумажные носители, не справляясь в полной мере со своими функциями, постепенно вытесняются электронными, вследствие чего проблема конфиденциальности информации становится более актуальной. Информация нуждается в защите, ее сохранности и безопасности.

Безопасность информации определяется некоторыми критериями. Выделяются три основные принципа информационной безопасности:

1. Целостность информации. Необходимость обеспечить защиту информации от сбоев, которые приводят к повреждению информации или ее полному уничтожению

2. Конфиденциальность информации. Информация должна быть недоступна для посторонних пользователей.

3. Доступность информации. С другой стороны, информация должна быть доступна для авторизированных пользователей.

Итак, хранение информации организации должно быть организовано таким образом, чтобы соблюдались вышеперечисленные принципы. Каким образом этого добиться и что препятствует их выполнению?

Организация, имея огромное количество информации, увеличивающееся непрерывно с каждым днем, сталкивается с угрозами, которые могут нанести вред имеющимся данным. Все существующие угрозы разделяют на две группы: внутренние и внешние.

Данная классификация дает нам понимание того, где находится злоумышленник, который может воздействовать на ресурсы организации как удаленно (используя всевозможные Интернет-ресурсы), так и получать доступ к информации организации через ее прямые источники, имея возможность использовать архив или иные конфиденциальные ресурсы.

Невероятно разнообразны возможности воздействия на информационную безопасность с помощью вредоносного программного обеспечения:

1. Проникновение разрушающих программ (компьютерные вирусы, программы вида «червь» или «троянский конь»).

2. Несанкционированное чтение, копирование, распространение либо удаление информации.

3. Блокирование работы пользователей системы программными средствами.

4. Анализ и последующая ликвидация существующего ПО.

5. Раскрытие, перехват и хищение секретных кодов и паролей.

6. Внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений.

7. Похищение информации с внешних носителей.

Внутренние угрозы информационной безопасности представляют собой гораздо более опасный фактор. Существует классификация сотрудников, наносящих неизгладимый урон сохранности информации предприятия, которые осуществляют свою деятельность по определенным причинам:

1. Сотрудники – мстители. Эти работники имеют личные корыстные цели отомстить предприятию по причине увольнения, сделанного выговора или просто иных личных интересов.

2. Сотрудники – спекулянты. Ищут выгоду за счет ресурсов компании-работодателя. Такие работники пытаются вести нечестную игру, используя секретные данные предприятия, разработки стратегического планирования и т.д.

3. Сотрудники – шпионы. Считается наиболее опасным типом внутренних злоумышленников, так как зачастую такие агенты являются членами преступных группировок. Такие сотрудники заранее продумывают свою деятельность, достигают высот в карьере в короткие сроки, в связи с чем легко добиваются доступа к особо конфиденциальной информации.

Однако стоит заменить, что злоумышленные атаки со стороны сотрудников случаются реже, чем случайные потери информации по причине неосторожности персонала или обычной компьютерной безграмотности.

Каждая отдельная организация поразному обеспечивает информационную безопасность. В зависимости от рода деятельности, масштабов и прочих индивидуальных особенностей, руководством компании принимается решение о применении той или иной стратегии для обеспечения безопасного пользования компьютерными сетями, формируется политика компании в области защиты информации. Основой для создания целостной системы является документ. В нем сформулированы все принципы политики организации в области обеспечения безопасности информации. Данный документ включает в себя следующие вопросы:

1. Правовое обеспечение защиты информации: государственные законы и акты, внутренние нормативные и организационные документы компании, например, устав, правила внутреннего распорядка, инструкции для сотрудников о коммерческой тайне.

2. Определение и перечисление потенциальных угроз безопасности информации. Они могут быть связаны с деятельностью человека, с нарушениями нормальной работы технического обеспечения или со стихийными бедствиями независящими от человека.

3. Конкретизация данных, подлежащих защите.

4. Создание специального отдела по вопросу защиты информации. Служба безопасности компании отвечает за разработку политики защиты информации, выполнение организационных мер, а в обязанности ИТ-подразделений входит работа с программными и аппаратными средствами.

Сформировав политику и обозначив необходимые задачи, компания проводит организационные мероприятия, связанные с защитой информации.

Во-первых, разрабатываются инструкции и регламенты для сотрудников.

Во-вторых, должное внимание должно быть уделено охране территории и помещений. Для этого во многих компаниях уже введена система пропускного режима. В помещения, где размещены серверы автоматизированного управления и вовсе ограничивается доступ. Определенный объем документации все же остается на бумажных носителях, их предлагается хранить в специально защищенных местах, например, в сейфах. При этом ненужные носители необходимо ликвидировать сразу после использования. Установка мониторов компьютеров, клавиатуры, принтеров проводится таким образом, чтобы исключить возможность просмотра или копирования информации посторонними лицами. Особое внимание необходимо уделять жестким дискам и компьютерам, которые отправляются в ремонтные службы – информация с них должна быть удалена прежде, чем устройство станет доступно постороннему лицу. Для обеспечения более высокого уровня безопасности, проведение регулярных проверок по соблюдению всех правил, положений и инструкций является необходимым.

Для защиты от внешних интернет угроз необходимо использовать системы предотвращения вторжений на уровне хоста (HIPS). Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации (например, антивирусного пакета) обеспечивают очень высокий уровень. При учете всех мер, организация получает защиту практически от всех типов вредоносного ПО, работа хакера, решившего попробовать пробить информационную защиту предприятия, значительно затрудняется. В таком случае сохраняется вся интеллектуальная собственность и важные данные организации.

В заключение хотелось бы сказать, информационная безопасность – неотъемлемая часть любого предприятия, будь то маленькая фирма или крупная корпорации.

В данной статье мы кратко и понятно объяснили, как бороться с несанкционированными входами в операционную систему организации, как защититься от угроз. Таким образом, достигли поставленной цели. Не стоит забывать, что, вовремя не подумав о безопасности, организация может понести огромный ущерб, к которому относятся прямые финансовые убытки, удар по репутации, потеря клиентов, снижение конкурентоспособности.

Таким образом, обеспечение информационной безопасности компании имеет вполне конкретный экономический смысл.

Список литературы

1. Бармен Скотт. Разработка правил информационной безопасности. – М.: Вильямс, 2002. – С. 208.

2. Справочно-правовая система «Консультант Плюс».

3. Хачатурова С.С. Информационные технологии в юриспруденции: учебное пособие. // Фундаментальные исследования. – 2009. – № 9. – С. 8–9.

4. Хачатурова С.С. Организация предпринимательской деятельности. Создание собственного дела // Международный журнал экспериментального образования. – 2012. – № 2. – С. 137–138.

5. http://www.abc-people.com/typework/economy/e-confl-8.htm.

6. http://www.epam-group.ru/aboutus/news-and-events/articles/2009/aboutus-ar-gaz-prom-09-01-2009.html.

7. http://www.nestor.minsk.by/sr/2007/07/sr70713.html.

8. http://www.safensoft.ru/security.phtml?c=791.

9. Kaspersky.ru. Режим доступа: http://www.kaspersky.ru/about/news/business/2012/Zaschita_dlya_Titana_Laboratoriya_Kasperskogo_obespechivaet_bezopasnost_Korporaciya_VSMPO-AVISMA.

10. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – С. 544.