УДК 004.056.5

Информационная безопасность предприятия

Строков К.А., студент
Кузнецова Т.В., старший преподаватель
кафедры «Экономика и финансы»
ФГБОУ ВО «Пензенский государственный университет»
e-mail:t.v.kuznetsova.penza@yandex.ru
Россия, Пенза

Информационная безопасность предприятия – это состояние защиты корпоративных данных, которая помогает обеспечить целостность, конфиденциальность, аутентичность и доступность. В основном на многих предприятиях компьютеры и прочая компьютерная техника является лишь частью информационной системы. Но при этом огромное влияние оказывают на защиту информации, которая как раз передается при помощи компьютера.

Информация (от лат. Information – разъяснение, осведомлённость) – сведения об окружающем мире. Если информацию рассматривать как товар, можно в принципе понять, что обеспечение информационной безопасности приведет к экономии средств, в то время как вред, нанесенный ей, приводит к материальным расходам. Например, выявление технологии производства уникального продукта приведет к возникновению подобного продукта, однако от иного производителя, и как результат несоблюдение информационной безопасности, владелец технологии, потеряет часть рынка.

Полная информационная безопасность компаний предполагает постоянный контроль в реальном времени абсолютно всех значимых событий и состояний, оказывающих большое влияние на безопасность информации. Защита обязана осуществляться круглосуточно и ежегодно и охватывать весь жизненный цикл данных – от её поступления либо формирования вплоть до ликвидации либо утраты актуальности. На уровне компании за информационную безопасность отвечают отделы информационных технологий, финансовой безопасности, сотрудников и прочие работы. [1]

Успех производственной и предпринимательской деятельности в небольшом количестве зависит в умения распоряжаться информацией и использовать можно лишь ту информацию, которая нужна рынку, но не известна ему. Защите подлежит та информация, которая имеет ценность для предпринимателя, то есть при определении ценности предпринимательской информации важно соблюдать критерии такие, как своевременность, достоверность поступивших сведений и полезность. Существует довольно много угроз обеспечения информационной безопасности предприятия.

Главным объектом воздействия угроз безопасности подвергается та информация, которая обрабатывается в автоматизированных системах. Основанием автоматизированных систем считают: программные оболочки, программы общего назначения, текстовые процессоры, общесистемное программное обеспечение, редакторы. В основном, информация в автоматизированной системы поступает с рабочего места локальной сети. К пользователям автоматизированной системы относятся все

зарегистрированные в ней лица, наделенные определенными полномочиями доступа.

Источники угроз безопасности информации предприятия делятся на три группы: стихийные, антропогенные и техногенные.

К стихийным источникам угроз относят землетрясения, пожары, ураганы и др.

К антропогенным источникам угроз относят: злонамеренных конкурентов и партнеров, криминальные структуры.

В техногенные источники угроз входят: средства связи и сигнализации, некачественные технические и программные средства обработки информации, а также другие технические средства, которые применяются в организации.

Направления, которые помогут защитить информацию в организации:

- Организационно-техническое направление, в рамках которого создается оболочка вокруг объекта защиты, т.е. информационных ресурсов, с определенной степенью надежности исключающая или существенно затрудняющая проведение манипуляций с информацией в автоматизированных системах против интересов пользователей системы;
- Правовое направление, сосредоточенное на создание иммунитета, основанного на угрозе применения репрессивного инструмента в отношении нарушителей интересов пользователей системы, и устанавливающее механизм применения санкций в отношении правонарушителя;
- Экономическое направление, предусматривающее механизм устранения материального ущерба, причиненного собственнику информации в результате несанкционированных действий с ней со стороны правонарушителя.

Организационно-технические направление защиты данных считается более реальным направлением в защите данных компании. [2]

Вопрос информационной безопасности становится краеугольным камнем в деятельности организации. Утечка информации может привести к серьезным проблемам для компании – от значительных финансовых убытков до полной ликвидации. Чаще всего “утекают” из компаний документы финансового характера, технологические и конструкторские разработки, логины и пароли для входа в сеть других организаций. Но из-за чего чаще всего возникают угрозы информационной безопасности?

1) Невнимательность и халатность сотрудников. (Всегда есть возможность, что кто-нибудь откроет «фишинговое» письмо и внедрит вирус на сервер компании или, например, скопирует файл с конфиденциальными сведениями на планшет или флэшку.)

2) Использование пиратского программного обеспечения. (Иногда руководители компаний пытаются сэкономить на покупке лицензионного программного обеспечения. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов.)

3) Вирусы. (Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак.)

4) Угрозы со стороны совладельцев бизнеса. (Именно легальные пользователи — одна из основных причин утечек информации в компаниях. Такие утечки специалисты называют инсайдерскими, а всех инсайдеров условно делят на несколько групп:

- «Нарушители» — среднее звено и топ-менеджеры, позволяющие себе небольшие нарушения информационной безопасности — играют в компьютерные игры, делают онлайн-покупки с рабочих компьютеров, пользуются личной почтой.
- «Преступники» — чаще всего инсайдерами являются топ-менеджеры, имеющие доступ к важной информации и злоупотребляющие своими привилегиями. Они самостоятельно устанавливают различные приложения, могут отсылать конфиденциальную информацию заинтересованным в ней третьим лицам и т.д.
- «Кроты» — сотрудники, которые умышленно крадут важную информацию за материальное вознаграждение от компании-конкурента.
- Еще одна категория — это уволенные и обиженные на компанию сотрудники, которые забирают с собой всю информацию, к которой они имели доступ.)

Хотя количество угроз постоянно растет, появляются все новые и новые вирусы, увеличивается интенсивность и частота DDoS-атак, разработчики средств защиты информации тоже не стоят на месте. На каждую угрозу разрабатывается новое защитное программное обеспечение или совершенствуется уже имеющееся. Среди средств информационной защиты можно выделить:

- Физические средства защиты информации. (К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами.)
- Базовые средства защиты электронной информации. (К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции.)
- Анти-DDoS (Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик.)
- Резервное копирование данных. (Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров.)

- План аварийного восстановления данных. (Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании для того, чтобы в максимально сжатые сроки устранить риск простоя.)[3]

Итак, защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.

Список литературы:

1) Обеспечение информационной безопасности предприятия [Электронный ресурс]. URL: https://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html (дата обращения: 21.12.2018)

2) Информационная безопасность предприятия [Электронный ресурс]. URL: https://studme.org/1120061121678/ekonomika/informatsionnaya_bezopasnost_predpriyatiya (дата обращения: 21.12.2018)

3) Информационная безопасность предприятия: ключевые угрозы и средства защиты [Электронный ресурс]. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (дата обращения: 21.12.2018)