ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БИЗНЕСЕ

С.В. КАРПЕНКО, Т.А. ЗАЯЦ,
Гомель, Беларусь, БТЭУ

Информационная безопасность — это состояние защищённости информационной среды. Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Рост числа правонарушений в сфере компьютерной информации идет не менее быстрыми темпами, чем компьютеризация в Республике Беларусь.

Эффективность информационной защиты бизнеса можно определить на основе подсчета возможных предотвращенных потерь.

По данным [1] в 2014 г. в Республике Беларусь было выявлено 8739 компьютерных преступлений, из которых было раскрыто 96%.

За первое полугодие 2014г. в Беларуси выявили 4 тыс. 295 преступлений в сфере высоких технологий. Злоумышленники, действующие в "компьютерной" сфере криминала, - это молодые люди в возрасте до 18 лет, 58% - от 18 до 25 лет, причем около 70% из них имеют высшее либо незаконченное высшее образование.

Основная часть преступлений, с которыми приходится иметь дело - это компьютерные преступления, связанные с незаконным доступом к информации и с использованием вредоносных программ. Было отмечено, что оперативники управления довольно успешно борются с подобными видами преступлений.

Согласно статистике, процент раскрываемости противоправных деяний в сфере высоких технологий составляет 96%. Самое громкое преступление раскрытое "компьютерными" сыщиками – поимка 7 хакеров, которые украли у 8 тыс. владельцев банковских пластиковых карт около 21 млн. долл. На территории России проведена операция по задержанию группы "хакеров", которые с использованием вредоносных программ осуществляли атаки на серверы банков и букмейкерских компаний в Великобритании. Злоумышленники требовали у потерпевших за прекращение противоправных действий от 5 тыс. до 50 тыс. долл. В настоящее время находятся под арестом двое из подозреваемых. Им вменяется в вину 273 случая (изготовление и распространение вредоносных компьютерных программ) и 163 (вымогательство) [1].

Актуальность безопасности информации в современных условиях:

1. Закон Республики Беларусь от 10.11.2008 N 455-З (ред. От 04.01.2014) «Об информации, информатизации и защите информации»

В главе 3. Правовой режим информации имеется 6 статьи об информационной безопасности.

В главе 4. Распространение и предоставление – 4 статьи [2].

2. Кодекс Республики Беларусь от 09.07.1999 N 275-З (ред. От 24.10.2014) "Уголовный кодекс Республики Беларусь"

В главе 31. Преступления против информационной безопасности – 7 статей про компьютерную информацию [3].

Политика безопасности — это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации. Только человек, четко осознающий цели организации и условия се функционирования, может определить, какую информацию необходимо защищать и насколько существенными могут стать потери от несанкционированного распространения, искажения или разрушения информации.

Защита информационных ресурсов (данных) компании от утечек – важнейшая задача мероприятий по информационной безопасности. При любом виде деятельности у каждой компании есть определённый набор сведений, которые являются основой существования фирмы. Эти сведения и обслуживающий их документооборот являются коммерческой тайной компании, и, разумеется, требуют защиты от утечек и разглашения. Угрозы утечки данных разделяют на два направления: внешние (вредоносное ПО, хакерские атаки и т.д.) и внутренние угрозы (инсайдеры). Эффективная защита информации от утечек требует комплексного подхода. Для успешного построения системы информационной безопасности требуется анализ и аудит информационной безопасности предприятия.

SafenSoft предлагает сбалансированную защиту от утечки данных, разработанную специально для среднего и малого бизнеса. Комплекс строит защиту, которая не нарушает текущие алгоритмы документооборота в компании, но в то же время сохраняет информацию от неавторизованного доступа, копирования или изменения. Не пустить лишних людей к важным данным, защитить информацию от взлома и заражения извне, исключить оплошности при работе с информацией, дать возможность полного контроля и мониторинга действий сотрудников – по этим принципам созданы продукты для информационной безопасности бизнеса SysWatch Enterprise Suite и DLP Guard. В них реализован весь необходимый функционал по предотвращению утечек информации, а небольшая стоимость и простота внедрения делают продукты SafenSoft идеальным выбором для компаний, которые стремятся сделать свой бизнес эффективным и безопасным [4]. Источники нарушений безопасности: ошибки пользователей и персонала; атака извне; обиженные сотрудники; нечестные сотрудники; вирусы; проблемы физической безопасности [5].

Угрозы информационной безопасности предприятия совершенно реальны, их нельзя недооценивать. Кроме противодействия внешним угрозам особое внимание следует уделить угрозам внутренним. Важно помнить, что утечки корпоративных секретов случаются не только по злому умыслу – как правило, их причина в элементарной халатности и невнимательности работника. При выборе

средств защиты следует строить надёжную модульную систему безопасности, закрытую от рисков вторжения извне и позволяющую осуществлять контроль и мониторинг за потоком информации внутри компании [6]. Внедрение мер обеспечения ИБ включает Безопасность серверов и рабочих станций, Защиту от утечек конфиденциальной информации, Управление правами доступа к информации, Безопасность корпоративных бизнес-приложений, Безопасность WEB-ресурсов, Безопасность корпоративных порталов, Безопасность электронной почты, Безопасность удаленного доступа к корпоративным ресурсам, Безопасность использования мобильных устройств. Идентификация, аутентификация и управления правами доступа, Криптографическая защита информации. Контроль носителей информации, Противодействие мошенничеству и гарантирование дохода и др [6].

Правовые мероприятия - создание в организации нормативной правовой базы по информационной безопасности, т.е. разработка на основе законодательных актов РБ необходимых руководящих и нормативно-методических документов, перечней охраняемых сведений, мер ответственности лиц за нарушение порядка работы с конфиденциальной информацией.

Список литературы:

1. Петров, А.А. Компьютерная безопасность: криптографические методы защиты // А.А. Петров, 2014. – с.250.
2. Закон Республики Беларусь от 10.11.2008 N 455-З (ред. От 04.01.2014) «Об информации, информатизации и защите информации»
3. Кодекс Республики Беларусь от 09.07.1999 N 275-З (ред. От 24.10.2014) "Уголовный кодекс Республики Беларусь"
4. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. – М.: ДМК Пресс, 2010. – 544 с.
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. Пособие. – М.: ИД «ФОРУМ»: ИНФРА – М, 2011. – 416 с.
6. Ярочкин, В.И. Информационная безопасность: Учебное пособие для вузов. М.: Академический проект, 2006 – 4-е изд. – 544 с.