Пецевич Л. И.
БГЭУ (Минск)

ФИРМЕННЫЙ СТИЛЬ В ДЕЯТЕЛЬНОСТИ ФИРМЫ

Три небольшие фирмы – «Альянс», «Веминко» и «Надежда» образовали страховую компанию (СК) «АльВеНа». Уже более десяти лет «АльВеНа» занимается практическим страхованием, участвует в становлении страхового бизнеса Беларуси.

Для того чтобы клиенты и партнеры смогли «узнать» СК «АльВеНа» в совокупности альтернативных предложений, она имеет свой фирменный стиль.

Девиз компании: « Наши клиенты – это самое важное достояние».

Логотипом фирмы является ее наименование - «АльВеНа», которое одновременно выступает товарным знаком (знаком обслуживания).

Фирменный блок фирмы представляет собой сочетание изобразительного товарного знака «АльВеНы» и логотипа. Фирменный блок содержат соответствующим образом оформленные бланки писем, страховые полисы, правила компании.

Слоган «АльВеНы» содержит основные принципы деятельности компании, ее кредо, и выглядит следующим образом:

АльВеНа -- РеАльная
уВеренность
в Настоящем

У «АльВеНы» два основных фирменных цвета – серый и зеленый. Они присутствуют в товарном знаке компании. Кроме того, буклеты, календари, ручки, указатели, стенды оформляются в данной цветовой гамме.

Пилютик А. А.
Институт экономики НАН Беларуси (Минск)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Когда проектировался Интернет, никто и не думал о безопасности. Интернет разрабатывался для исследовательских целей, и доступ был открыт всем желающим. И только в последнее время, когда количество пользователей достигло миллионов, появилась серьезная обеспокоенность по поводу безопасности информации.

Есть два типа потенциальных нарушителей – это хакеры и шпионы. Хакером руководит любопытство или злой умысел. Они способны нанести значительные повреждения, которые могут вывести из строя

информационные системы. Промышленный шпионаж – это сбор информации о позиции продукта, о клиентах, просмотр форумов потребителей, кража секретов компании.

Несанкционированное использование корпоративной сети – наиболее часто встречающаяся форма нарушения безопасности. Аутентификация пользователя и шифрование данных с использованием брандмауэров, в общем, могут предотвратить несанкционированный доступ. Иногда "злоумышленник" может попытаться обойти защиту, притворяясь авторизованным пользователем.

Первое что должна сделать любая организация для защиты от хакерской атаки, это убедится в том, что политика безопасности на местах четко определена, осуществима и оформлена документально. Кроме того, в политику безопасности должно войти письменное информирование пользователя об ответственности. А поскольку необходимо обеспечить и доступность, и целостность, и секретность данных, то политика безопасности определяет доступ в сеть, доступ к услугам, аутентификацию локального и удаленного пользователя, возможность установить связь в обоих направлениях, шифровку данных и дисков, меры по защите от вирусов и обучение персонала. Необходимо принять все меры безопасности для предотвращения вторжения, краж информации и "отказов от предоставления услуг". Политика безопасности должна быть подчинена стратегическим целям компании, т.е. определять основные линии защиты: защищать ли все данные по умолчанию, гарантировать ли доступ лишь конкретным пользователям, защищать лишь некоторые данные или предоставить открытый доступ.

Будущее электронной коммерции – это такие брандмауэры, которые защищают сетевой доступ, но не защищают информацию при передаче зашифрованных данных через Интернет. Для обеспечения сквозного канала безопасности разрабатываются схемы, гарантирующие передачу криптографически защищенных потоков. В последнее время появились новые концепции, такие как аутентификация на основе сертификатов и новые продукты. Эти средства позволяют идентифицировать серверы и защищать транзакции на всем пути прохождения пакетов. Цифровой сертификат выполняет ту же роль, что и лицензия водителя или диплом врача: он подтверждает, что его обладатель имеет соответствующую квалификацию.