

# Знать, чтобы предотвращать

*В настоящее время, когда все без исключения организации используют информационные системы для передачи, хранения и обработки информации, очень велика вероятность утечки конфиденциальных данных. Говоря другими словами, кража важной информации, халатность сотрудников, саботаж, атаки хакеров могут нанести очень существенный удар как по финансам, так и по имиджу любой компании. Предотвратить риски поможет грамотно проведенный аудит информационной безопасности.*

## Знание - сила

Если мы хотим предотвратить какое-то нежелательное для нас действие, мы должны понимать, как это действие происходит. Чтобы бороться с утечками конфиденциальных данных, необходимо, прежде всего, идентифицировать каналы утечки информации. Но если специалистам по информационной безопасности нужно для этого время, то внутренние нарушители уже знают, как можно украсть необходимый им документ. Поэтому наиболее важный вопрос информационной безопасности: "Как именно происходит утечка информации?" Ответ на этот вопрос сможет дать аудит информационной безопасности.

Аудит информационной безопасности — это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с критериями информационной безопасности. Важно понимать, что это не единовременное мероприятие, а регулярный процесс, который должен проводиться с заданной периодичностью. Многие руководи-

тели организаций заблуждаются, думая, что, проведя один раз аудит информационной безопасности, выявив каналы утечки информации и приняв соответствующие меры по нейтрализации этих каналов, они полностью обеспечат защиту корпоративной информационной системы. Это не так, ведь современные технологии не стоят на месте, а развиваются очень быстро, соответственно технологии хакерских атак и способы кражи конфиденциальных данных тоже совершенствуются.

Поэтому проводить аудит информационной безопасности необходимо регулярно.

## Голые факты

По результатам исследования, проведенного аналитическим центром компании "InfoWatch", наибольшее количество утечек (50%) произошло через ноутбуки, КПК, USB-флэшки, CD и DVD-диски и др. Малые размеры носителей информации, помимо всех очевидных преимуществ, имеют и менее

заметный недостаток – эти устройства очень легко потерять или спрятать. В результате непреднамеренной потери носителя конфиденциальная информация оказывается у неизвестных людей, которые распоряжаются ею по своему усмотрению. В то же время внутренние нарушители легко спрячут маленький носитель и вынесут конфиденциальные данные за пределы организации.

Следующий канал утечки информации – это Интернет (12%). Но Интернет, в отличие от мобильных устройств, не позволяет быстро передавать большие объемы данных. Кроме того, достаточно легко поймать внутреннего нарушителя и доказать его вину, если использовать сетевую фильтрацию.

Еще 5% случаев нарушения информационной безопасности произошло из-за неправильной утилизации или потери резервных носителей. По 3% пришлось на электронные послания и факсы, а также на почту. 17% случаев нарушения внутренней информационной безопасности произошло по другим каналам. В 10% случаев так и не удалось выяснить, каким образом была произведена кража конфиденциальной информации.

Основная причина нарушения внутренней информационной безопасности – невыполнение или выполнение не надлежащим образом требований должностных инструкций, политик безопасности (если они разработаны), распоряжений либо пренебрежительное отношение к простым средствам защиты информации. Например, потери ноутбуков происходят достаточно часто. И хотя по правилам организации незащищенных мобильных компьютеров быть не должно, все равно утерянные ноутбуки содержат конфиденциальную информацию в незашифрованном виде. Все вышесказанное еще раз подчеркивает, что внутренние нарушители могут быть в любом коллективе.

### О том, что важно знать

Руководителю организации важно знать, что аудит информационной безопасности поможет его организации избежать материального ущерба, связанного с кражей конфиденциальной информации, а также нематериальных потерь, таких как репутация организации, потеря деловых партнеров и клиентов. Другими словами, грамотно проведенный аудит информационной безопасности поможет снизить риски организации и увеличить уверенность в собственной системе безопасности. Кроме того, организации, которые предостав-

ляют услугу проведения аудита информационной безопасности, должны иметь большой опыт и безупречную репутацию, в противном случае высока вероятность предоставления некачественной услуги.

Руководителю отдела информационных технологий важно знать, что аудит информационной безопасности даст ему перечень каналов утечки информации в организации, рекомендации по нейтрализации этих каналов, перечень угроз и оценку рисков по каждой угрозе. А также поможет сформировать необходимый комплекс защитных мероприятий и разработать план внедрения этих мероприятий.

Большинство руководителей отделов информационных технологий заблуждаются, считая, что они смогут провести аудит информационной безопасности собственными силами. Такой аудит не обеспечит объективного результата. Ведь сотрудники организации, участвующие в проведении аудита информационной безопасности, зачастую не имеют соответствующей квалификации. Кроме того, они могут скрыть некоторые каналы утечки информации, чтобы самим ими воспользоваться. К этому добавляется самоуверенность многих сотрудников отделов информационных технологий, которая заключается в том, что если они разрабатывали и в данный момент осуществляют поддержку корпоративной информационной системы, то эта система полностью защищена, и ни о каких каналах утечки информации и речи быть не может.

### Надежный партнер

Компания "Арт-мастер" работает на IT-рынке Украины уже более 7-ми лет. В 2005 году компания получила сертификат соответствия системы менеджмента качества требованиям международного стандарта ISO 9001:2000, а в 2006 году, впервые в Украине, система менеджмента информационной безопасности компании была сертифицирована на соответствие требованиям международного стандарта ISO/IEC 27001:2005 "Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

Сегодня компания "Арт-мастер" остается единственной компанией в Украине, которая сертифицирована на соответствие требованиям международного стандарта ISO/IEC 27001:2005. Представительства компании "Арт-мастер" открыты во всех регионах Украины, что дает возможность качественно и в короткие сроки предоставлять услуги аудита ин-

формационной безопасности по всей территории Украины.

Компания "Арт-мастер" имеет лицензии Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины (с 2007 года Государственная служба специальной связи и защиты информации Украины) на проведение деятельности в сфере технической защиты информации всех видов, в том числе информации, которая содержит государственную тайну, и криптографической защиты информации, в том числе конфиденциальной информации, которая принадлежит государству.

Одним из основных направлений деятельности компании является обеспечение информационной безопасности, в рамках этого направления предоставляются услуги по проведению аудита информационной безопасности.

Аудит информационной безопасности от "Арт-мастер"

Компания "Арт-мастер" предоставляет услуги по проведению аудитов информационной безопасности следующих видов:

- экспертный аудит информационной безопасности;
- аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005.

В ходе экспертного аудита информационной безопасности выявляются недостатки в системе информационной безопасности организации на основе опыта экспертов, участвующих в процедуре аудита.

Основными документами, которые регламентируют порядок проведения экспертного аудита информационной безопасности, являются нормативные документы Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины, а с 2007 года и нормативные документы Государственной службы специальной связи и защиты информации Украины.

Результатом экспертного аудита информационной безопасности является общая оценка защищенности корпоративной информационной системы организации, основывающаяся на анализе рисков и перечне обнаруженных уязвимостей. По результатам аудита формируется отчет и разрабатываются рекомендации для нейтрализации выявленных уязвимостей.

Стандарт ISO/IEC 27001:2005 представляет собой перечень требований к системе менеджмента информационной безопасности, обязательных для сертификации. Стандарт устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совер-

шенствованию документированной системы менеджмента информационной безопасности в контексте существующих бизнес-рисков организации.

Проводить аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 могут только высококвалифицированные специалисты, которые прошли обучение и получили сертификат аудитора. Сотрудники компании "Арт-мастер" сертифицированы как аудиторы по международному стандарту ISO/IEC 27001:2005 и имеют большой опыт работы в этой области.

По результатам аудита на соответствие международному стандарту ISO/IEC 27001:2005 руководитель организации получает описание области действия системы менеджмента информационной безопасности, реестр важных активов, методику оценки рисков, отчет по оценке рисков, критерии принятия рисков, а также список политик, руководств, процедур и инструкций, необходимых для функционирования системы менеджмента информационной безопасности.

Аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 будет интересен любым коммерческим организациям, в том числе и тем, которые собираются работать на международном рынке.

Клиентами компании "Арт-мастер" являются государственные органы, которые находятся во всех регионах Украины и имеют сложные распределенные информационные системы. Также клиентами компании "Арт-мастер" являются коммерческие организации, которые используют корпоративные информационные системы любой сложности, начиная от одной рабочей станции или ноутбука и заканчивая сложными территориально-распределенными информационными системами, насчитывающими сотни рабочих станций и десятки серверов.

Подытоживая вышесказанное, отметим, что аудит информационной безопасности просто необходим современным, быстрорастущим организациям, так как только он сможет обеспечить своевременное идентифицирование каналов утечки информации и, как следствие, своевременное реагирование и принятия решений по обеспечению безопасности корпоративной информационной системы организации. Вовремя проведенный аудит информационной безопасности поможет избежать ущерба любого вида и размера.

*По материалам компании "Арт-Мастер"*