



# Система В СООТВЕТСТВИИ С ЗАКОНОМ

*Компания «Информзащита» разработала и внедрила комплексную систему информационной безопасности в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам (Роспатент) и головном подведомственном учреждении — Федеральном институте промышленной собственности в соответствии с требованиями закона «О персональных данных»*

## Технические решения плюс процессы

Современный уровень угроз безопасности информации, отсутствие контроля над инцидентами информационной безопасности, а также большой объем работ по управлению учетными записями, связанный с множеством разнородных автоматизированных систем, поставили задачу создания адекватной защиты информационных ресурсов Роспатента. Кроме того, остро стояла задача приведения в соответствие с требованиями Федерального закона № 152-ФЗ «О персональных данных» и требованиями государственных регуляторов защищенности автоматизированных систем Роспатента, обрабатывающих персональные данные.

Эта система защиты создавалась не только путем развертывания определенных технических средств защиты, но и за счет использования выстроенных под конкретную деятельность ведомства процессов управления информационной безопасностью. Для проектов в области ИБ второе направление в настоящий момент все-таки не является стандартной практикой. Именно это стало одним из примечательных моментов проекта.

Для осуществления проекта был проведен открытый конкурс по выбору исполнителя, по результатам которого победителем была признана

компания «Информзащита». Перед специалистами этой компании поставили важное условие — требование учитывать при проектировании систем информационной безопасности уже использующиеся в Роспатенте системы защиты информации, а также внедрять системы информационной безопасности с постоянным присутствием сотрудников подразделения безопасности Роспатента в режиме обучения и обмена опытом.

## Описание решения

Материальная основа корпоративной информационной системы Роспатента — десятки единиц серверного оборудования и тысячи персональных компьютеров функциональных пользователей, многие из которых подключены к сети Интернет для решения производственных задач. Кроме того, используется широкий спектр сетевого и телекоммуникационного оборудования различных типов и производителей, широко применяются сетевые принтеры и сканеры, а также специализированные средства информационной безопасности. С учетом этого все решения и продукты, входящие в комплексную систему информационной безопасности, обеспечивают необходимое взаимодействие и поддерживают централизованное администрирование.

На первом этапе работ в Роспатенте было проведено обследование, чтобы определить класс систем, обрабатывающих персональные данные, установлены актуальные угрозы безопасности и сформулированы требования к обеспечению безопасности персональных данных. Разработаны частные модели угроз для информационных систем персональных данных и внутренние документы, регламентирующие процессы обработки и обеспечения безопасности персональных данных в соответствии с действующим законодательством Российской Федерации.

На втором этапе проектировались и внедрялись программные и программно-аппаратные средства, обеспечивающие управление учетными записями пользователей, отвечающие за предотвращение атак, анализ защищенности и управление инцидентами. Все установленные системы незамедлительно принимались на техническое обслуживание и сопровождение департаментом сервиса компании «Информзащита» в режиме 24×7.

Чтобы нейтрализовать угрозы компьютерных атак, внедрены системы обнаружения атак и анализа защищенности, которые были реализованы на основе программного обеспечения компании IBM ISS RealSecure и Internet Scanner, создающего защиту от атак в реальном времени с высокой производительностью. Помимо внедрения программной части, были осуществлены монтаж и настройка всей необходимой аппаратной базы — серверов и управляющих рабочих станций, обеспечивших круглосуточную и бесперебойную работу всей системы.

Проблема отсутствия централизованного управления учетными записями пользователей и автоматического назначения необходимых прав доступа была решена с помощью продукта IBM Tivoli Access Manager. Реализация этого решения привела к сокращению издержек на работы по управлению учетными записями и доступом, а также обеспечила контроль над учетными записями пользователей на протяжении всего жизненного цикла. В то же время повысилась эффективность работы пользователей, которым теперь не нужна многократная аутентификация при доступе к различным приложениям.

Внедрена подсистема управления инцидентами информационной безопасности на базе высокопроизводительной системы мониторинга и корреляции событий ArcSight Enterprise Security Management. Сотни тысяч событий в день создавали массу проблем специалистам по информационной безопасности. Внедрение ArcSight ESM позволило реализовать централизованный сбор, хранение, обработку и мониторинг событий ИБ в режиме реального времени. За счет этого сократилось время выявления, реагирования и

расследования инцидентов безопасности, что, в свою очередь, способствовало снижению рисков и повышению устойчивости бизнес-процессов ведомства. Помимо основного функционала, ArcSight ESM укомплектована дополнительными пакетами, обеспечивающими предоставление отчетности по стандарту ISO 17799 и противодействие инсайдерам. Специалистам Роспатента предоставлен программный пакет (SDK), позволяющий самостоятельно расширять область контроля системы ArcSight ESM на новые приложения и ресурсы.

Для предотвращения несанкционированного доступа к персональным данным было внедрено средство защиты информации Secret Net совместно с электронным замком «Соболь» производства компании «Код безопасности».

Дальнейшее развитие проекта предусматривает расширение комплексной системы информационной безопасности на менее критичные и локальные информационные системы и ресурсы Роспатента, а также повышение осведомленности сотрудников Роспатента в вопросах ИБ.

### Что в итоге

Разработанная система информационной безопасности позволила достичь качественно нового уровня функционирования подсистем защиты информации, позволяющего им обеспечивать конфиденциальность, целостность и доступность обрабатываемой информации. Были разработаны необходимые внутренние документы, а также внедрены технические средства обеспечения безопасности, что позволило привести все информационные системы организации в соответствие с требованиями Федерального закона «О персональных данных» и положений нормативных документов ФСТЭК РФ и ФСБ РФ по обеспечению безопасности персональных данных.

Сейчас специалисты компании «Информзащита» занимаются техническим сопровождением информационных систем Роспатента.

## РОСПАТЕНТ

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент) — федеральный орган исполнительной власти, предоставляющий правовую охрану на объекты интеллектуальной собственности, а также осуществляющий контроль и надзор в сфере правовой охраны и использования объектов интеллектуальной собственности. Роспатент находится в ведении Министерства образования и науки Российской Федерации.