



Елена Некрасова/  
Elena.Nekrasova@computerra.ru/

# Экономия без риска



Меры, необходимые для приведения ИСПДн организации в соответствие с требованиями 152-ФЗ, требуют затрат, в некоторых случаях — существенных. Возможно ли достичь максимальной защищенности персональных данных, затратив минимальные ресурсы, прежде всего финансовые?



**В**се расходы оператора персональных данных на обеспечение их защиты делятся на прямые и косвенные. К прямым относятся, например, затраты на создание информационной системы персональных данных (ИСПДн) в защищенном исполнении, поставка и настройка соответствующих аппаратно-программных средств защиты информации, расходы на персонал, на аттестацию и декларирование АС и пр. Сюда же можно причислить разработку модели угроз, адаптированной под конкретную бизнес-модель. Важной частью статьи затрат является проектирование и обследование. «Проект, как правило, предусматривает проведение аудита инфраструктуры и информационных систем обработки персональных данных, технические и организационные мероприятия по реализации средств защиты ПДн, аттестации объектов защиты, — уточняет Андрей Бугаенко, ИТ-директор национального оператора связи «Синтерра».

Косвенными считаются затраты на эксплуатацию, аттестацию (если необходимо) и поддержку средств защиты персональных данных. Сюда же относятся и дополнительные расходы, связанные с последующей эксплуатацией систем и управлением изменениями в них, затраты на персонал и специалистов в области юриспруденции, информационных технологий, защиты информации и т. д.

Самыми крупными статьями затрат оператора ПДн являются расходы на организационные меры и на технические средства защиты. Затраты на персонал, лицензии и прочие расходы, как правило, существенно меньше. Соотношение этих составляющих и их

абсолютная величина зависят от многих факторов, ключевыми из которых являются

- > размер оператора персональных данных и объем обрабатываемых ПДн;
- > наличие в штате специалистов по защите информации; опыт защиты информации ограниченного доступа (других видов тайн);
- > наличие средств защиты, сертифицированных по требованиям защиты ПДн;
- > степень понимания руководством организации необходимости защиты ПДн;
- > наличие в компании юристов, имеющих опыт работы в области защиты персональных данных (большая редкость).

«В среднем суммарные затраты на организационные меры для оператора в 100–200 рабочих мест при привлечении внешних исполнителей составляют от 1 до 2 млн руб., а на технические средства защиты — от 2 млн», — отмечает Алексей Сабанов, заместитель генерального директора компании Aladdin.

## Можно расходовать меньше

На какие направления деятельности в рамках внедрения и поддержки ИСПДн необходимо обратить внимание, чтобы снизить расходы? Прежде всего эксперты советуют уделить внимание самому первому этапу жизненного цикла создания системы. «Ошибки в классификации ИСПДн (в частности завышение класса) существенно влияют на все последующие затраты, — объясняет Сергей Петренко, эксперт в области непрерывности бизнеса



и информационной безопасности компании «АйТи». — Ошибки, допущенные на первом этапе, могут необоснованно увеличить стоимость проекта в 3–5 раз». Следовательно, начинать надо с анализа потребности в обработке ПДн и связанных с этим рисков, с выработки и оформления принципиальных решений по характеру и масштабам обработки и накопления персональных данных. «От этого часто зависит класс защиты, устанавливаемый для ИСПДн, а иногда — границы системы обработки, — отмечает Андрей Филинов, системный архитектор по информационной безопасности компании IBM в России и СНГ. — Это, в свою очередь, влияет на число и сложность требуемых мер и средств защиты, на строгость процессов контроля, приводит к росту затрат».

При выборе способов снижения расходов на защиту ПДн необходимо учитывать влияние всех сторон, вовлеченных в проект. «Дело в том, — объясняет Алексей Сабанов, — что, согласно сегодняшним требованиям, уже не только оператор ПДн и интегратор, внедряющий решение, но и разработчик информационной системы обязаны предоставить сервисы защиты обрабатываемых персональных данных. Исходя из этого, стоимость решения и последующей его сервисной поддержки зависит от слаженного взаимодействия этих трех сторон. При этом оператору не удастся «отсидеться» и остаться в стороне: ему надо во все вникать и по возможности самому возглавлять все работы».

Необходимо тщательно проработать архитектуру будущей ИСПДн и изучить бизнес-процессы обработки данных.

— На этом этапе снижение расходов возможно лишь за счет использования предыдущего опыта построения и внедрения, — уве-

рен Денис Андриков, заместитель технического директора по работе с заказчиками компании «Открытые Технологии». — Без этого оператор похож на слепого,двигающегося на ощупь, шаг за шагом все дальше уходящего в неизвестность. Вопрос «А вдруг я сделаю что-нибудь не так?» приобретает все большую актуальность: ведь защищают одни, а проверяют соответствие другие. Если вплотную подойти к вопросам внедрения и поддержки, то необходимо обратить внимание на поддержку производителя: возможности сертификации оборудования, регулярные обновления программных комплексов, гибкость в доработках функционала, широкую матрицу совместимости.

Таким образом, отмечает Алексей Сабанов, правила снижения рисков и последующих расходов очень просты:

- > внимательное отношение к формированию модели угроз с целью минимизации класса ИСПДн и режима обработки ПДн, что в итоге снизит стоимость систем защиты;
- > предоставление пользователям самых минимальных прав доступа, достаточных только для выполнения служебных обязанностей;
- > персонализация доступа с помощью строгой аутентификации и обеспечение неотвратимости наказания в случае нарушений;
- > создание развитой системы мониторинга действий пользователей и аудита систем защиты;

## Самыми крупными статьями затрат оператора ПДн являются расходы на организационные меры и на технические средства защиты.

- > использование сертифицированных и проверенных многолетней практикой средств защиты.

### Классы данных

Снизить затраты оператора ПДн можно за счет оптимизации категорий обрабатываемых ПДн, их разумного сегментирования и обезличивания. «В первую очередь необходимо обратить внимание на определение класса ИСПДн, — предупреждает Андрей Бугаенко. — От степени и глубины понимания действующего законодательства и правил, от точного их исполнения зависит объем расходов. Зачастую один сотрудник оператора ИСПДн, глубоко разбирающийся в тонкостях закона и подзаконных актов в области защиты персональных данных, может в разы снизить затраты на проект. Ни для кого не секрет, что на рынке совсем немного подрядчиков, которые готовы поставить заказчику максимально эффективное решение, а не максимальный набор услуг, которые они умеют оказывать».

Андрей Филинов советует действовать по существующей инструкции: снижать количество единиц хранения ПДн в системе и степень подробности накапливаемых сведений, вводить алиасы для субъектов учета.

Для начала следует проанализировать необходимость обработки персональных данных для деятельности компании. «Может быть, исторически бизнес складывался так, что в рамках взаимодействия записывались паспортные данные субъекта ПДн, — рассказывает Денис Андриков. — Например, при получении дисконтной карты в розничном магазине. На самом же деле использовался

лишь адрес для отправки корреспонденции и ФИО. Однако в таком способе снижения затрат может скрываться куда БОльшая затратная статья, чем защита ПДн, а именно — перестройка бизнес-процессов».

С технологической точки зрения оптимизировать затраты можно за счет обезличивания ПДн. Фактически информационной системой персональных данных станет централизованная база данных, а клиентская часть будет обрабатывать унифицированные идентификаторы и безликие таблицы. Существенного эффекта при таком подходе можно достичь на распределенной базе данных с большим количеством рабочих мест и транзакций на обработку. «За счет асинхронной обработки информации, — рассказывает Андрей Бугаенко, — можно оказаться от характеристики распределенности обработки данных. Результата можно добиться дроблением

## Ошибки в классификации ИСПДн (в частности завышение класса) существенно влияют на все последующие затраты.

■ **Сергей Петренко:** Надо четко идентифицировать критически важные бизнес-процессы и обеспечивающие ИТ-сервисы



информационных систем или их независимых компонентов. Если совместить этот процесс с оптимизацией бизнес-процессов в целом и развитием ИТ в компании, синергетический эффект может быть весьма значителен».

Наконец, как это ни парадоксально, один из важных моментов по возможному снижению затрат — отказ от автоматизированной обработки части персональных данных.

### Организационные и технические меры

Как определить оптимальный состав применяемых организационных и технических мер обеспечения безопасности ПДн? «Это самый сложный, но вместе с тем и самый интересный вопрос, — считает Сергей Петренко. — Своего рода лакмусовая бумажка для исполнителей в области защиты данных. Определить оптимальный состав возможно, если иметь четко сформулированные требования, критерии и показатели защищенности, а самое главное — типовые решения по защите ПДн, согласованные с регуляторами. На практике обоснованную оптимизацию мер защиты могут предлагать только единичные компании-интеграторы с большим опытом работы в области защиты информации».

Денис Андриков советует прежде всего досконально изучить требования регуляторов, разобраться в нормативных документах, понять, какие внесены изменения в требования. Далее — изучить правоприменительную практику, понять методику проверки. Если бизнес-процессы, в которых задействована обработка ПДн, не регламентированы, то необходимо проанализировать деятельность и выявить соответствующие активности, провести разделение на основе вовлеченности автоматизированных средств в процесс об-

работки. После этого можно сформулировать оптимальный состав организационных мер. Для оптимизации технической архитектуры требуется определенный опыт системного интегратора, так как в этом процессе обычно задействованы обученные и сертифицированные специалисты, способные быстро и качественно спроектировать и внедрить необходимый комплекс программно-технических средств защиты.

Очевидно, что оптимальный состав определяется, исходя из особенностей конкретной организации. Операторы персональных данных имеют разные масштабы бизнеса, обрабатывают различные ПДн, разнятся по опыту в области защиты информации и ПДн, что и влияет на выбор тех или иных организационных и технических мер. Кроме того, в организации уже могли быть внедрены какие-либо средства защиты информации. В случае если эти средства можно применить для защиты ПДн, оператору не потребуется приобретать дополнительное оборудование и нести дополнительные расходы.

— Допустим, в штате имеются грамотные специалисты по информационной безопасности, сформирована концепция защиты информации ограниченного доступа, есть утвержденная модель угроз, работающая система управления информационной безопасностью, внедрены сертифицированные средства защиты, — приводит пример Алексей Сабанов. — В этом случае



■ **Алексей Сабанов:** Нужны средства защиты от нежелательных действий администраторов, разработчиков и аудиторов



■ **Андрей Филинов:** Активное применение алиасов для субъектов ПДн помогает снизить уровень требований по защите

для соответствия требованиям по защите ПДн достаточно будет провести минимум дополнительных организационных мероприятий и подготовить небольшое количество документов.

### Структура и процессы обработки

Оптимизация структуры ИСПДн и процессов обработки данных — еще один источник снижения расходов оператора. Здесь не обойтись без детального обследования деятельности компании. Сергей Петренко советует четко идентифицировать критически важные бизнес-процессы и обеспечивающие ИТ-сервисы: «Можно порекомендовать использовать методологию описания бизнес-процессов организации NGOSS, выявлять и ранжировать информационные потоки и собственно защищаемые информационные ресурсы. В основном это возможно только в компаниях и организациях третьего-четвертого уровня зрелости (по методологии COBIT 4.1 и 5.0, ITIL V3) с соответствующими метриками и способами измерения и оптимизации уровня защищенности операторов персональных данных».

В процессе обследования необходимо изучить фактическую потребность в ПДн при ведении бизнеса и по возможности

## ■ Баланс между затратами и размером возможного ущерба

■ **Иван Бурдело,**  
директор департамента  
информационной безо-  
пасности компании «КА-  
БЕСТ» группы «Астерос»



**П**ри создании и модернизации информационных систем персональных данных важно ??? между затратами на применяемые меры и средства защиты и размером возможного ущерба от реализации актуальных угроз безопасности ПДн.

Существует несколько способов снижения затрат на защиту персональных данных. Один из них — оптимизация процессов обработки ПДн, позволяющая исключить как избыточность самих ПДн, так и лишние звенья в технологии их обработки. Тем самым можно уменьшить количество точек защиты и, как следствие, удешевить создание системы защиты персональных данных. Зачастую в ИСПДн обрабатываются персональные данные, которые содержат информацию о состоянии здоровья, национальности и пр. От использования этой информации компания вполне может отказаться, вынести за общую технологию обработки информации или обрабатывать ее без использования средств автоматизации. Это приводит к понижению класса ИСПДн и, соответственно, к уменьшению расходов на защиту информации. Другим, не менее эффективным и распространенным способом снижения затрат является перевод ИСПДн из категории «типовой» в «специальную». Для типовой системы определены и четко зафиксированы требования по обеспечению безопас-

ности ПДн, которые зачастую избыточны и повышают затраты на их защиту. Для специальных ИСПДн эти требования формируются на основе индивидуальной для каждой системы модели актуальных угроз. Такая модель угроз учитывает специфику деятельности конкретной компании и сложившуюся технологию обработки информации. Она также позволяет объективно оценить существующие риски реализации тех или иных угроз безопасности ПДн, разработать подходящую концепцию защиты, обосновать выбор соответствующих мер по защите ПДн и тем самым сократить расходы на излишние средства. Минимизировать затраты также можно путем «легализации» (с точки зрения требований нормативных документов ФСТЭК и ФСБ России) использования существующих средств защиты через процедуры их сертификации. На основе анализа полноты и достаточности реализованных мер защиты устанавливается их соответствие требованиям по обеспечению безопасности ПДн. В этом случае заказчику не нужно приобретать дополнительные средства защиты, дублирующие уже имеющийся функционал. Среди действенных путей снижения расходов на создание и поддержку СЗПДн — опти-

мизация архитектуры самой ИСПДн, которая направлена на исключение из процесса обработки информации определенного количества субъектов и объектов доступа. ИСПДн — это люди, технологии и защищаемая информация. Чем меньше составляющих вовлечено в процесс обработки ПДн, тем меньше область защиты. Поэтому наиболее эффективными мерами является локализация мест хранения данных, обезличивание их или внедрение специальных технологий доступа к информации. Такие решения могут стать выходом для клиента, если он владеет системой, которая в числе других задач выполняет обработку персональных данных на нескольких средствах вычислительной техники — например, в отделе кадров. В этом случае для обработки ПДн необходимо выделить сегмент локальной вычислительной сети со своим коммуникационным оборудованием, серверами и рабочими станциями, обеспечить его должными мерами защиты. А в остальной части информационной системы можно использовать обезличенные или общедоступные персональные данные. В нашей практике были проекты, когда мы использовали подобный подход, чтобы снизить затраты на построение системы защиты ПДн. Это решение позволило сократить стоимость проекта в несколько раз. Однако при проектировании ИСПДн не стоит забывать, что средства защиты не должны влиять на бизнес-процессы организации и существенно ограничивать функциональность других информационных систем компании.

Система защиты ПДн должна быть прозрачна для конечного пользователя.

Значительной статьей затрат оператора ИСПДн являются расходы на персонал. Зачастую предприятия ограничены собственными ресурсами. Поэтому создание ИСПДн — и особенно такую важную, задачу, как проектирование, — лучше доверить специализированной компании. Дополнительный плюс обращения к экспертам в том, что они берут на себя техническое и правовое сопровождение во время проведения проверок контролирующими органами. Возможно, это и не принесет прямой экономии, однако в соотношении с репутационными рисками и возможными санкциями такая схема работы — наиболее разумна и эффективна.

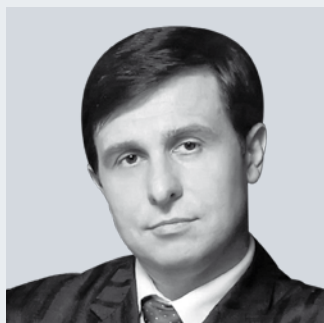
Какой вариант будет выбран — определяется требованиями бизнеса. Главное, чтобы система исправно работала и выполняла свою ключевую функцию по поддержке бизнеса. ◀

убрать их из тех участков операционного процесса, где они не нужны, отделить такие «стерилизованные» части системы от остальных частей. «В итоге меры защиты потребуются не для всей системы, а лишь для отдельных ее частей, — объясняет Андрей Филинов. — Активное применение алиасов для субъектов ПДн помогает снизить уровень требований по защите. При грамотном применении таких вполне законных уловок можно иногда добиться ситуации, когда данные, прикрытые алиасами, вообще перестают быть предметом обработки в сетевой многопользовательской среде без ущерба для бизнеса и его клиентов. Не всегда легко бывает добиться признания регуляторами этого факта и допустимости такого решения. Но за него стоит бороться: оно же позволяет экономить». Андрей Бугаенко приводит пример такого решения: «Можно свести распределенную структуру ИСПДн второго класса к набору взаимодействующих в дискретном режиме обмена информацией систем третьего класса. Ряд простых и действенных приемов по оптимизации интерфейсов программных средств и разграничению доступа к информационным системам может стать удивительно эффективным».

Есть способы оптимизации, основанные на технологиях, в частности на виртуализации. Стоит рассмотреть и аутсорсинг как возможное решение в части архивного хранения больших объемов ПДн.

## ■ Уделите внимание сертификации

■ **Михаил Романов,**  
директор по развитию  
бизнеса компании  
Stonesoft в России,  
СНГ и странах Балтии



**В**ыбор сертифицированных средств защиты для ИСПДн имеет свои нюансы. Их много, но часто между сертификатами на разные средства, выполняющие практически одинаковые функции, нет никакого соответствия. Для примера возьмем перечень требований к межсетевым экранам для многопользовательских ИСПДн с подключением к сетям общего пользования. Если их проанализировать, то легко обнаружить, что среди них есть требования по наличию функций трансляции сетевых адресов, идентификации и аутентификации администратора при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации, требования оперативного восстановления

свойств экранирования после сбоев и отказов, которые являются характерными для межсетевых экранов второго класса защищенности в соответствии с РД МЭ. Поэтому даже наличие у меж сетевого экрана сертификата по третьему классу защищенности формально недостаточно для применения в таких ИСПДн. Часто сертификация средств защиты, в особенности иностранного производства, осуществляется партиями. Чем плоха такая схема сертификации на практике? Тем, что через некоторое время будет установлена уже не та

## Модель угроз

Выбор системы защиты персональных данных определяется теми угрозами, которые могут быть реализованы для ПДн в данной организации. Модель угроз является одним из основополагающих документов, на базе которого строится система защиты персональных данных (СЗПДн). Стоимость разработки модели угроз не занимает гигантскую долю в цене всего проекта. Есть ли смысл разрабатывать модель угроз индивидуально — или стоит предпочесть типовую?

Большинство экспертов в области защиты персональных данных сходятся во мнении, что «типовых» ИСПДн не существует. Так или иначе, все системы в жизни индивидуальны и по большому счету могут быть отнесены по требованиям ФСТЭК к категории «специальных». «Использование модели угроз по шаблону — это ошибка, относящаяся к классу системных, — уверен Сергей Петренко. — Модель угроз безопасности для конкретной организации всегда сугубо индивидуальна. По этой причине к разработке модели угроз и соответствующей модели нарушителя нужно подходить сугубо индивидуально». Тем не менее с целью снижения затрат на разработку можно использовать типовую отраслевую модель как «нулевой» или базовый вариант, а затем совершенствовать ее, исходя из своей специфики. Для минимизации рисков новичкам лучше поручить это специализированному лицензиату ФСТЭК.

версия продукта, на которую выдан сертификат, а не устанавливать обновления, выпускаемые производителем, означает подвергнуть свою информационную систему серьезному риску. За проведение же процедуры инспекционного контроля после выхода каждой новой версии продукта придется заплатить дополнительно. Таким образом, при выборе средств защиты лучше все же предпочесть те, в сертификате которых явно сказано о возможности их применения в ИСПДн соответствующего класса и по возможности сертифицированных по схеме сертификации производства. Stonesoft как производитель средств сетевой защиты старается дать достойный ответ на все перечисленные проблемы. В настоящий момент компания завершает процесс сертификации всех своих решений по требованиям безопасности информации ФСТЭК России по схеме

сертификации производства, что позволит эффективно решить проблему перехода на новые версии продуктов. StoneGate Firewall будет сертифицирован по второму классу защищенности для межсетевых экранов, система предотвращения вторжений StoneGate IPS и шлюз защиты удаленного доступа StoneGate SSL — по третьему классу. Все продукты, включая версии для защиты в виртуальной среде, будут сертифицированы по четвертому уровню контроля НДВ. Кроме того, в StoneGate Firewall и StoneGate SSL встроена поддержка сертифицированных криптографических продуктов Крипто Про. В настоящее время также ведутся работы по обеспечению сертификации обоих продуктов в системе сертификации ФСБ России. Таким образом, решения StoneGate можно применять для защиты информационных систем персональных данных до класса К1 включительно. ◀

— Возможно, — размышляет Андрей Филинов, — массовым бизнес-структурам, занятым схожими видами деятельности (например, страховым компаниям, медучреждениям, учебным заведениям), стоит подумать о создании, одобрении регуляторами и официальном распространении «типовых моделей» в пределах своей отрасли. Но вот обобщение на уровне выше, чем отраслевые модели, пожалуй, нереально. Выбор варианта модели угроз, не соответствующего фактическим условиям оператора, скорее всего, в перспективе увеличит издержки оператора. В одном случае он переплатит за меры защиты, которые для него избыточны, в другом — будет оштрафован за ущерб, возникший вследствие недостаточности мер защиты.

## Архитектурные решения

Существует два диаметрально противоположных подхода к проектированию архитектуры ИСПДн: централизованная и распределенная обработка. Очевидно, что для конкретного оператора оптимальным будет особый принцип построения, однако можно выделить несколько универсальных свойств. Опыт большинства проектов, реализованных в 2009–2010 годы, показывает, что идеальной архитектурной моделью является создание защищенного узла хранения и обработки ПДн на базе дата-центра с предоставлением пользователям терминального доступа. «При этом необходимо предусмотреть дополнительные средства защиты от нежелательных действий администраторов, разработчиков и



■ **Денис Андриков:** Необходимо досконально изучить требования регуляторов, разобраться в нормативных документах



■ **Андрей Бугаенко:** В первую очередь необходимо обратить внимание на определение класса ИСПДн

аудиторов, — предупреждает Алексей Сабанов. — Такие средства защиты уже представлены на рынке. Рассмотренная модель обладает безусловными преимуществами, так как не требует значительных вложений при построении ИСПДн и ее сопровождении». В альтернативном варианте для реализации распределенной модели ИСПДн с «толстым» клиентом необходимо будет защитить, (а возможно, и аттестовать) каждое рабочее место. Очевидно, что это очень дорогой вариант.

«Централизация обработки снижает операционные затраты при наличии широкой региональной сети, — рассказывает Денис Андриков. — В этом случае отсутствует необходимость аттестации отдельно взятых представительств. Распределенная обработка ПДн будет выгоднее для случая, когда имеют место ограничение на каналы связи и жесткие требования по консолидации всей базы ПДн. В общем, можно сказать, что стоимость проекта защиты распределенной ИСПДн будет выше при общих равных условиях, однако резервы снижения стоимости кроются во внедрении общей информационной шины, которая даст выигрыш в цене на большом объеме внедрения за счет стандартизации региональных ИСПДн».

«Один из способов снижения затрат на внедрение системы защиты ПДн — это выбор модели поэтапного внедрения систем защиты, в том числе Data Leak Prevention — защиты от утечек информации, в частности ПДн, с рабочих станций сотрудников компаний, — рассказывает Сергей Вахонин, директор по информационным технологиям ЗАО «Смарт Лайн Инк». — Соответственно, необходимо DLP-решение корпоративного уровня, которое благодаря своей модульной архитектуре позволит построить полноценную функции защиты информации и ПДн от базового уровня контроля устройств и портов к более мощному сочетанию контроля портов, устройств и сетевых коммуникаций с возможностями контентного анализа. Такое архитектурное решение позволит добиться экономии как на человеческих ресурсах (снижается число специалистов, задействованных на внедрении системы в целом, за счет их

## От степени и глубины понимания действующего законодательства и правил, от точного их исполнения зависит объем расходов.



■ **Сергей Вахонин:** Снизить затраты на внедрение системы защиты ПДн поможет модель поэтапного их внедрения

поэтапного привлечения), так и на общей стоимости решения и его поддержки».

При оценке перспективных затрат Андрей Филинов советует как можно внимательнее относиться ко всему, что связано с жизненным циклом защищаемых массивов персональных данных: «Время последующего существования информационного актива — это самый недооцениваемый фактор в большинстве расчетов. Впрочем, кто-то может принять стратегию немедленного избавления от всех критичных данных, потребность в которых отпала».

Экономия достигается в основном за счет того, что расходы и риски перекладываются на кого-то другого — к примеру, на тех, кто экономит за счет большого масштаба деятельности. «Если закон обязывает хранить ПДн клиентов десять лет, но доступ к данным фактически не нужен уже через пару недель после завершения обслуживания клиента — отдайте такие данные из филиала в центральный архив, там их хранение обойдется дешевле», — рекомендует Андрей Филинов.

## Персонал

Одна из статей расходов оператора ПДн — затраты на персонал. Каким организациям имеет смысл обеспечивать безопасность ПДн силами собственного персонала, а каким — привлекать сторонние специализированные компании? Как показывает практика, далеко не всегда для построения системы защиты требуется привлечение аутсорсинговых фирм: все зависит как от наличия в собственном штате компании квалифицированных специалистов, так и от качества внедряемых систем, их интуитивной понятности, качества документации и развитости службы технической поддержки. «На

мой взгляд, любому, даже небольшому, оператору ПДн необходимо отправить на обучение технологиям защиты персональных данных хотя бы одного сотрудника, — считает Алексей Сабанов. — Это обеспечит существенную экономию как при постановке задачи привлекаемым экспертам по ИБ, так и при приемке работ аутсорсера. Кроме этого, обученный сотрудник сможет успешно взаимодействовать с контролирующими органами в ходе проведения проверок».

«Внедрение и поддержка ИСПДн собственными силами компаний приводит к очевидной экономии средств, — соглашается Сергей Вахонин. — Разумеется, речь идет прежде всего о технологическом внедрении при наличии четкого понимания стоящих перед инженерами и системными администраторами целей и задач. Выработку же стратегии внедрения, требований к функциональной части системы защиты ПДн имеет смысл поручить специализированным организациям, имеющим значительный опыт таких работ и знающих требования регуляторов».

Андрей Филинов подчеркивает:

— Своими силами справятся те, кто уже имеет в составе своей ИС действующие средства и аттестованные ранее системы защиты

информации, составляющей коммерческую, банковскую тайну или содержащей иные конфиденциальные сведения. Их затраты чаще всего будут минимальны и сведутся к оформлению документации оператора ПДн. Всем остальным будущим операторам стоит начать с обращения к специалистам. Или — напрямую в территориальный орган регулятора, как того требуют подзаконные акты к 152-ФЗ.

Для крупных операторов, обрабатывающих большой объем ПДн, целесообразно большинство работ выполнять (или по крайней мере управлять) силами собственных сотрудников. Привлечение сторонних организаций будет оправданным для выполнения специфичных работ, которые не под силу самому оператору. При этом необходимо очень внимательно относиться к составлению договоров, особенно в части ответственности исполнителя.

В целом эксперты придерживаются мнения, что оптимальна смешанная стратегия использования как собственных ресурсов (инсорсинга), так и сторонних (аутсорсинга). «Сторонние организации эффективны в случае аналитического обоснования и технического проектирования, а для контроля и мониторинга систем защиты лучше использовать собственные ресурсы, — заключает Сергей Петренко. <

## ■ Главное — чтобы экономия не стала самоцелью

■ Юрий Черкас, руководитель отдела технической защиты информации компании ReignVox



Работы по построению системы защиты ПДн требуют привлечения квалифицированных специалистов, которыми оператор, как правило, не располагает. Одной из статей расходов в связи с этим становится стоимость услуг сторонних организаций, проводящих аудит информационных систем и процессов обработки персональных данных оператора, выполняющих работы по проектированию системы защиты, внедрению средств защиты и дающих рекомендации по изменению процессов обработки ПДн.

Опыт показывает, что для построения комплексной системы защиты очень редко оказываются достаточно имеющимися технических средств. Такая ситуация определяет еще одну статью расходов — закупка программных и аппаратных средств защиты информации.

Кроме того, в ходе создания системы защиты оператору часто приходится проводить реинжиниринг части бизнес-процессов и процедур, в рамках которых осуществляется обработка персональных данных, что требует определенных временных, человеческих и, как следствие, финансовых затрат.

Не менее значимая часть расходов приходится и на персонал, силами которого обеспечивается безопасность ПДн. Существует два варианта: обеспечение безопасности силами собственного персонала и привлечение сторонних специализированных организаций. Первый вариант используется опера-

торами, штатное расписание которых предусматривает подразделения, ответственные за ИБ. Если же должной компетенции у оператора нет, целесообразно привлечь организацию-лицензиата. Для оптимизации расходов в этом случае необходимо четко выделить те мероприятия, которые оператор может выполнить самостоятельно. Максимальная же экономия достигается, когда оператор при создании информационных систем (еще на этапе проектирования) учитывает необходимость выполнения требований по защите информации, тем самым закладывая в ее возможности функции обеспечения информации. Говоря об экономичном подходе к защите ПДн, операторы часто проводят зависимость между затратами и разработкой индивидуальной модели угроз или выбором типовой. Но сама взаимосвязь в данном случае выстроена неверно. Каждая информационная система оператора является индивидуальной. Перечень угроз безопасности, в том числе и

актуальных, зависит во многом от структуры информационной системы и реализованных организационных и технических мер по защите информации в целом. Более того, если целью построения системы защиты является не видимость защищенности, а реальная безопасность, то модель угроз предпочтительно разрабатывать для каждой конкретной системы с учетом уязвимостей ее ИТ: инфраструктуры и процедур обработки ПДн и уже реализованных мероприятий по защите информации. Бездумная, не подтвержденная оценочно-исследовательской деятельностью экономия в процессе реализации проекта по защите ПДн зачастую влечет за собой построение неактуальных моделей угроз — а значит, создание нежизнеспособных систем защиты ПДн. Это создает риск значительных убытков в результате утечек конфиденциальной информации и повторных расходов на создание полноценно функционирующей системы защиты. <