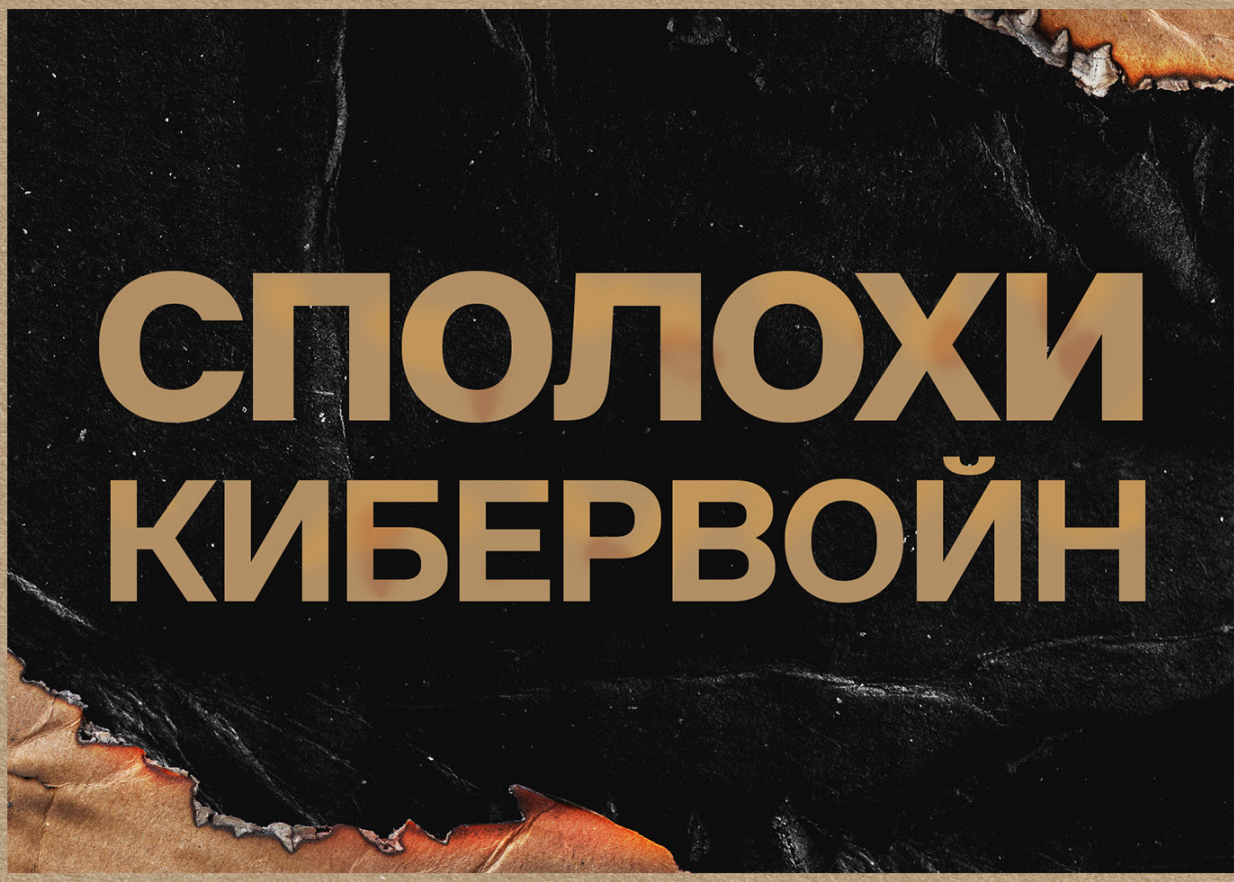
perimetrix

СПОЛОХИ КИБЕРВОЙН



КАДРЫ РЕШАЮТ ВСЕ *ИЛИ* ВНУТРЕННИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новости об инцедентах в сфере информационной безопасности у таких гигантов бизнеса, как Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Google, вполне могут лечь в основу остросюжетных блокбастеров с притягивающей зрителя ремаркой «Основано на реальных событиях». Ничего удивительного — вращающиеся там деньжищи способны спровоцировать корпоративные войны с коварными интригами, настоящими шпионами и высокопрофессиональными хакерами..

Но стоит ли опасаться всех этих джеймс–бондовских неприятностей руководству «заурядной» компании, в которой работа с персональными данными — «как у всех», нет «сведений, составляющих государственную тайну», а конкурентами являются не монстры хайтека, а себе подобные организации — заводы, проектные институты, торгово–производственные предприятия? Бояться — точно не стоит. Но задуматься и проницательно посмотреть на собственную компанию с точки зрения возможных информационных «свищей» нужно непременно.

Секреты, простые и сложные

«Секреты фирмы» есть почти у любой компании. Однако прежде чем начинать бороться с их утечками, нужно тщательно проанализировать, что же представляют собой тайны именно вашей компании. Есть ли вообще они у вас? Какая корпоративная информация имеет дополнительную ценность для вашего бизнеса, будучи скрытой от посторонних?

Являются ли ваши секреты «простыми» по своей форме? Можно ли их банально записать на бумажном листе или унести в голове, чтобы затем воспроизвести заинтересованной стороне? Или же это, наоборот, «сложные» секреты, которые существуют исключительно в форме трудновоспроизводимых данных и документов, созданных благодаря работе значительного числа людей и оттого еще более ценных?

Если секрет «прост» и может быть похищен сравнительно легким способом (просмотром, пересказом, переписыванием, фотографированием) — не тратьте усилий на сложные технические защитные меры. Они все равно не помогут. Нацельтесь на мониторинг действий сотрудников, так как они суть основной «коммуникационный канал» вашей компании с внешним миром и от их дисциплины и лояльности будет зависеть сохранность секретов.

А вот если ваши секреты представляют собой сложные информационные продукты (чертежи, проекты, материалы исследований, базы данных), которые могут утечь только по «техническим каналам связи», то неприкосновенность подобных ценных сведений может достигаться уже с помощью специализированных защитных средств. Причем, как это ни покажется странным, сложная форма вашего секрета может упростить задачу по его защите.

Запрещено все, что не разрешено

Самое важное, что должен сделать хозяин секрета (владелец компании, топ–менеджер), — это описать и внедрить «правильный» процесс работы с информацией ограниченного доступа.

Но не стоит поручать это IT–специалистам. Зачастую, не имея четкого представления о том, какие бизнес–задачи и рабочие процессы связывают сотрудников и ценную информацию в компании, они придерживаются принципа «не навреди» (а то и «моя хата с краю») и предоставляют самим сотрудникам право определять допустимые действия с ценными сведениями. Что, безусловно, не способствует информационной безопасности и порядку.

Ситуация не меняется, даже когда доступ к важным данным оставлентолько ограниченному числу сотрудников. Оставаясь вольными в своих действиях с ценной информацией, они неизбежно разбросают ее повсюду, потому что «им так удобнее».

Но как нельзя быть «немножко беременным», так и сведениям нельзя быть «немножко секретными». Надо четко усвоить, что в отношении корпоративных секретов допустим только один принцип: «*Запрещено делать всё, кроме того, что в явном виде разрешено*».

Приведенные коллегами «10 самых распространенных ошибок сотрудников, приводящих к утечке», имеют одну первопричину — отсутствие в организации порядка в бизнес–процессах и документообороте, неустроенность жизненного цикла ценных данных. И несмотря на повсеместное использование DLP, *кадры* по–прежнему остаются основным источником утечки данных.

90%

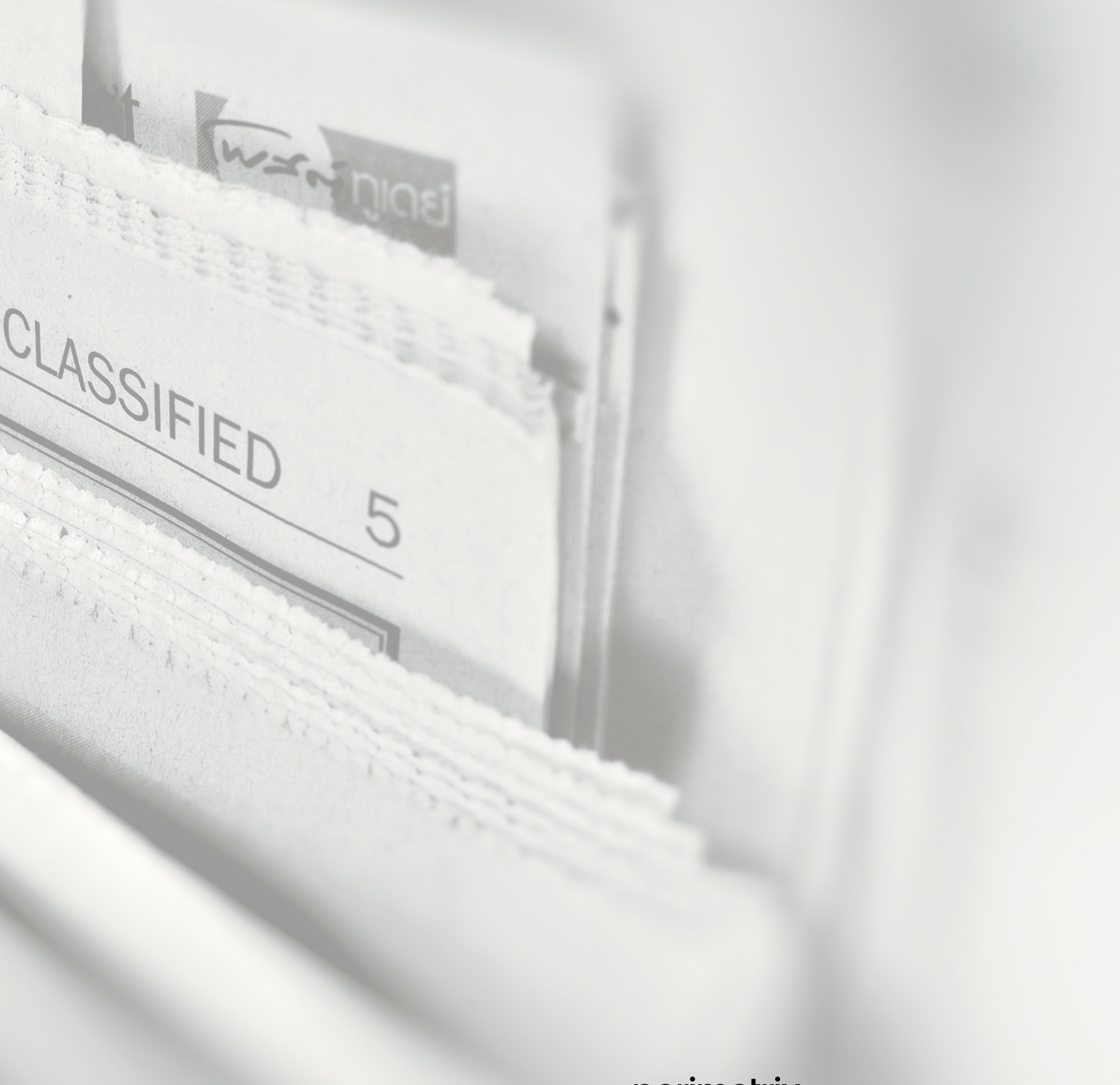
ДОЛЯ ИНЦИДЕНТОВ с конфиденциальными сведениями в 2019 г., приходящаяся на *умышленные* или *непреднамеренные* действия сотрудников[1]. ❶ Эта цифра почти не меняется год от года...

Начните с наведения порядка

— *дифференцируйте* и *классифицируйте* ценную информацию, чтобы отделить ее от «просто» информации, утечка которой не повлечет ущерба;
— определите, как должна создаваться, храниться, копироваться, вообще *двигаться* ценная информация в рабочих процессах;
— *определите* и *стандартизируйте*, насколько это возможно, основные бизнес–процессы, чувствительные к вопросам информационной безопасности;
— *минимизируйте* до необходимой и достаточной степени ознакомление сотрудников с секретными данными;
— *обучите* и впоследствии требуйте от сотрудников дисциплинированно придерживаться разработанных правил.

В результате этих мер вероятность «популярных» информационных угроз для вашей организации значительно уменьшится. ■

1 **ИСТОЧНИК** ↴ *Infosecurity Magazine*, 2019



perimetrix © 2021 Perimetrix LLC

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.

© COPYRIGHT. ALL RIGHTS RESERVED

ALL RIGHTS RESERVED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, INCLUDING PHOTOCOPYING, RECORDING, OR OTHER ELECTRONIC OR MECHANICAL METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF THE PUBLISHER, EXCEPT IN THE CASE OF BRIEF QUOTATIONS EMBODIED IN CRITICAL REVIEWS AND CERTAIN OTHER NONCOMMERCIAL USES PERMITTED BY COPYRIGHT LAW.