ZECURION
ANALYTICS

SuperJob

ОФИСНАЯ НЕБЕЗОПАСНОСТЬ

почему работники безнаказанно сливают информацию

www.zecurion.ru | analytics@zecurion.com | +7 495 221-21-60

Оглавление

Аннотация

Исследование компании Zecurion и портала Superjob.ru призвано выявить реальное отношение сотрудников к вопросам защиты корпоративной информации, поскольку в большинстве случаев именно человеческий фактор становится причиной утечек информации.

Важно, что участниками исследования являются обычные офисные сотрудники, непосредственно работающие с конфиденциальной информацией. Они могут дать больше объективных фактов, позволяющих судить о защищённости информации, нежели специалисты по безопасности, люди осведомлённые, но нередко обладающие уже замыленным взглядом.

В исследовании рассмотрены различные сценарии утечки информации. Ответы респондентов позволят понять, почему происходят утечки, как их можно минимизировать, какая информация наиболее уязвима, и, наконец, почему многочисленные инциденты происходят фактически безнаказанно.

Ключевые выводы

- Более половины работников (53%) подписывали соглашения о неразглашении конфиденциальных сведений при трудоустройстве, но это не мешает им передавать информацию вовне по незащищённым каналам и выносить документы на уязвимых мобильных носителях.
- Чтобы вынести информацию, чаще всего сотрудники пользуются флеэшками (49%) и электронной почтой (43%).
- Утечки информации происходят фактически безнаказанно, лишь в исключительно редких случаях (менее 1%) инсайдеров привлекают к уголовной ответственности.
- Наиболее ценными категориями информации в корпоративной среде, по мнению офисных работников, являются персональные данные сотрудников и клиентов (в сумме 28%), а также информация о сделках и договорах (16%).
- Только 10% топ-менеджеров считает, что их компаниям не нужны специализированные сотрудники или отделы, занимающиеся информационной безопасностью.

Методология исследования

Исследование проводилось путём online-опроса посетителей портала Superjob.ru в октябре-декабре 2012 года. В исследовании принимали участие только пользователи, зарегистрированные в базе данных резюме. Поэтому для каждого респондента имеется достоверная социально-демографическая карта.

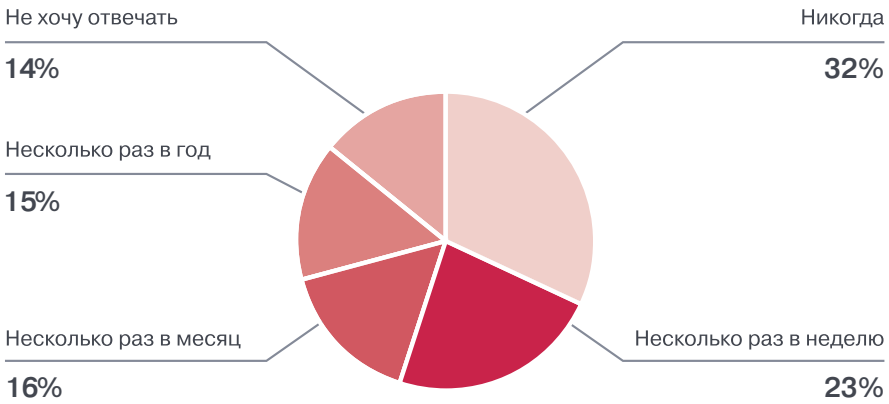
Для отбора участников использовался принцип случайного ненаправленного отбора. Это предполагает обращение к попавшему в выборку респонденту и его участие в многоэтапном опросе. Так как известны точные социально-демографические характеристики, то респонденту задавались только вопросы, непосредственно связанные с целью исследования.

Анкетирование проходило поэтапно, путём фильтров и квот, задаваемых в соответствии с задачами исследования. Опрос прекращался по достижении статистически оправданной базы численностью от 200 до 2000 человек для различных вопросов.

То, что плохо лежит

Для начала попытаемся понять, каким образом информация утекает. По статистике, наибольшее количество утечек происходит не по злому умыслу, а случайно, из-за невнимательности или вследствие низкой осведомлённости по вопросам защиты информации. Большое количество случайных утечек предопределяет отсутствие чётко прописанных политик и регламентов информационной безопасности. Сам характер обращения с данными в корпоративной среде угрожает их безопасности (см. рис. 1). Лишь треть офисных сотрудников никогда не работает с корпоративной информацией вне офиса. При этом 23% персонала, напротив, делают это постоянно, несколько раз в неделю.

Рисунок 1 ▶
Как часто сотрудники работают с корпоративной информацией вне офиса



Zecurion, Superjob, 2013

Среди тех, кто часто работает вне офиса, немало высокооплачиваемых сотрудников. Интересны их мнения на этот счёт. Главный бухгалтер из Зеленограда подтверждает, что работать на дому приходится «каждый день». Менеджер по развитию бизнеса из Тольятти считает, что «чтобы быть лучшим в отрасли, 40 часов в неделю мало»! А менеджер по работе с клиентам из Москвы сетует, что «хоть и не по закону, и не оплачивается, и неохота, но приходится работать всегда».

Если посмотреть, каким образом сотрудники получают доступ к корпоративной информации вне офиса (см. рис. 2), становятся понятными причины уязвимости данных. Информация уходит практически бесконтрольно. Особенно удручает использование сервисов файлообмена и высокая популярность мобильных накопителей (49% респондентов).

При использовании файлообменников пользователь фактически добровольно компрометирует данные. Любой, даже самый защищённый сервис, является публично доступным облаком. Каким образом защищается информация внутри облака, каковы внутренние процедуры обработки, где физически хранится информация, кто может получить к ней доступ — все эти и многие другие вопросы остаются открытыми. По данным исследования Lieberman Software, проведённого в ноябре-декабре 2012 года, 88% ИТ-специалистов считают, что данные, хранимые в облаке, могут быть потеряны, повреждены или украдены третьими лицами.

В качестве примера уязвимой системы файлообмена можно привести файловое хранилище Mail.ru, через которое, в частности, производится обмен файлами между пользователями ICQ. В середине января 2013 года

Рисунок 2 ▶

Каким образом сотрудники получают доступ к рабочей информации вне дома*

в интернете появилось описание уязвимости и скрипт для скачивания всех лежащих на серверах файлов. Тестовые запуски скрипта выявили большое количество информации и фотографий приватного характера, а также немало конфиденциальной информации, в том числе рабочие документы, накладные, бланки договоров, ведомости и т. д.

Усугубляет ситуацию и то, что на практике сотрудники пользуются не платными аккаунтами с некоторым декларируемым уровнем защиты, а простейшими сервисами, которые поисковые машины выдают в первую очередь. Эти сервисы зарабатывают деньги вовсе не на оказании услуг хранения файлов, а на показе пользователям рекламы сомнительного содержания. И потому не имеют особой заинтересованности в сохранении конфиденциальности передаваемой информации. Подобные сервисы вообще не предусматривают никакой защиты, так как никто не предполагал, что их будут использовать для передачи или хранения конфиденциальной информации.

Что касается мобильных накопителей (в частности, флэшек), их использование, на первый взгляд, более безопасно, поскольку к носителям никто, кроме владельца, не должен иметь доступ. Однако беспечность при использовании USB-накопителей может дорого стоить. По мировой статистике инцидентов за 2009-2012 годы, от 8% до 13% утечек происходит через мобильные накопители. Среди наиболее распространённых сценариев — кража или утеря флеэшки с данными. Сама по себе флеэшка не обеспечивает никакой безопасности, поэтому при их использовании исключительную важность приобретает применение шифрования. Хорошей практикой является также принудительное шифрование всех записываемых на мобильные накопители данных в прозрачном для пользователя режиме.

Среди комментариев, которые респонденты оставили в ответах на вопрос о способах передачи данных, обращает на себя внимание замечание одного из заместителей генерального директора крупной компании из Санкт-Петербурга об открытом доступе для него как топ-менеджера. То, что топ-менеджерам предоставляют доступ к информации в любое время из любого места, является серьёзной проблемой безопасности. Риски утечки в случае с топ-менеджерами очень высоки, поскольку руководители высокого ранга работают с информацией более высокого уровня. Поэтому регламент доступа к критически важной информации должен быть определён и неукоснительно соблюдаться, в первую очередь для первых лиц компаний.

* количество долей ответов превышает 100%, так как можно было выбрать несколько вариантов ответа

Своя рубаха ближе к телу

Одна из целей исследования состояла в выявлении наиболее ценной для компаний и самих сотрудников информации. Для этого были опрошены несколько категорий офисных работников, какую информацию, по их мнению, необходимо защищать. В сводной таблице (см. табл. 1) приведены наиболее популярные варианты ответов. Около 10% респондентов сообщили, что никакая информация не нуждается в защите, бизнес компании должен быть предельно прозрачным и открытым.

Таблица 1 ▶
Наиболее ценные категории информации

Категория	Бухгалтеры	Юристы	Менеджеры по продажам
Вся информация о компании, отсутствующая в открытом доступе	28%	25%	12%
Персональные данные собственных работников	7%	7%	9%
Клиентская база/ персональные данные клиентов	6%	19%	35%
Информация о зарплате сотрудников	24%	4%	4%
Информация о сделках, договорах	13%	13%	21%
Налоговая, бухгалтерская, управленческая отчётность	14%	7%	4%

Zecurion, Superjob, 2013

Различия в ценности различных типов информации для различных категорий сотрудников вполне объяснимы. Респонденты указывали наиболее важные именно для своей профессии классы данных. Именно поэтому категория «Налоговая, бухгалтерская, управленческая отчётность» получила так много голосов бухгалтеров и так мало голосов специалистов по продажам.

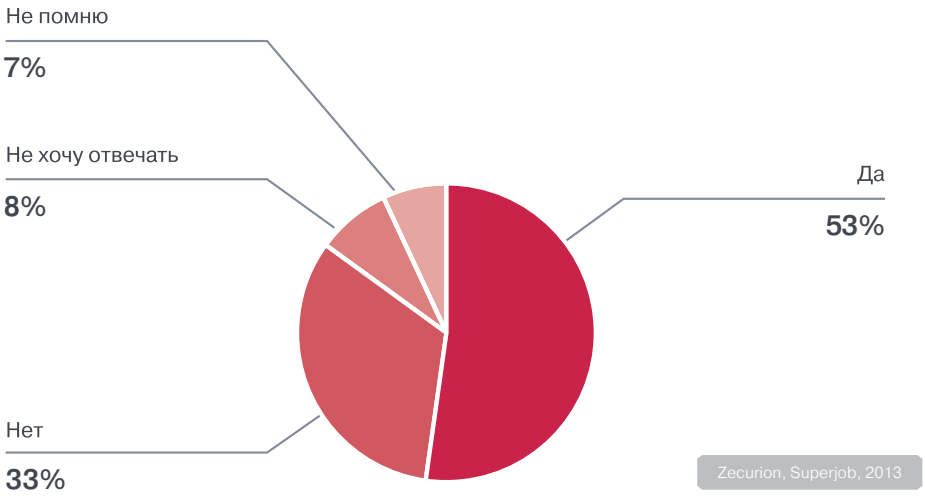
В то же время стоит отметить и общую тенденцию. Многие участники исследования говорят о необходимости защиты персональных данных сотрудников и клиентов. Даже несмотря на относительно небольшие размеры штрафов, которые компании платили за нарушение правил обработки персональных данных, требования №152-ФЗ и подзаконных актов остаются одними из основных мотиваторов для развития информационной безопасности во многих отраслях на протяжении последних 2-3 лет. В этом нет ничего удивительного, особенно если принять во внимание объявленное в конце 2012 года увеличение штрафов до 500 тыс. руб. для юридических лиц, и до 1 млн руб. в случае выявления повторного нарушения.

Организационные моменты

Так же, как театр начинается с вешалки, информационная безопасность организации должна начинаться на самых ранних этапах найма сотрудников. Одной из простейших, но в то же время эффективных мер, является подписание соглашения о неразглашении конфиденциальной информации или коммерческой тайны (NDA, non-disclosure agreement). Однако исследование показывает, что треть российских компаний (33%) пренебрегает этой мерой минимизации информационных рисков (см. рис. 3). В таких условиях сложно рассчитывать на более действенные процедуры, регулярные инструктажи, внедрение технических средств защиты информации. Между тем, простое уведомление сотрудника о том, что он работает с информацией ограниченного доступа, представляющей ценность для работодателя, позволит существенно сократить число непреднамеренных утечек.

Рисунок 3 ▶

Подписывали ли сотрудники соглашение о неразглашении информации?



В некоторых случаях, отмечают респонденты, работодатель требует подписку о неразглашении только с увольняющихся сотрудников. Такой документ тоже не будет лишним, однако, налицо нарушение рационального порядка действий. Во-первых, увольняющийся может просто-напросто отказаться подписывать бумагу, он в ней не заинтересован. Во-вторых, отсутствие подписанного соглашения о неразглашении подразумевает, что в течение действия трудового договора работник мог безнаказанно сливать информацию. Не слишком ли поздно беспокоиться о защите информации, когда человек уже решил покинуть компанию и, возможно, взял всю интересующую его информацию и нашёл вакансию у конкурента?

Самым необычным ответом на вопрос об NDA является сообщение начальника отдела маркетинга и продаж, который рассказал, что при трудоустройстве соглашение о неразглашении отказался подписывать… сам работодатель, «ссылаясь на открытость компании и надеясь на мою порядочность». Такое доверие, с одной стороны, заслуживает уважения, однако с другой стороны, может провести к самым печальным последствиям в случае недобросовестности сотрудника.

Степень ответственности

Какие же санкции предусмотрены за разглашение информации сотрудниками, подписавшими NDA? Чаще всего (30%) работодатель обещает применить дисциплинарную ответственность различной степени тяжести или наложить штраф (см. рис. 4). 18% компаний не прописывает ответственность вовсе. Отсутствие санкций снижает профилактический эффект от подписания документа.

Рисунок 4 ▶
Ответственность за разглашение информации

Zecurion, Superjob, 2013

Большое количество респондентов (24%) затрудняется ответить на вопрос. Косвенно, это указывает на недостаток внимания к вопросам информационной безопасности. Хотя рациональное объяснение забывчивости тоже имеется. При трудоустройстве приходится подписывать немало бумаг, а мысли нового сотрудника сосредоточены на прямых обязанностях, поэтому и большинство документов визируется не глядя.

В контексте данного вопроса интересно понять, какая же реально ответственность наступает в случае разглашения конфиденциальной информации. Респонденты называют всё те же штрафные и дисциплинарные (выговоры, «разъяснительные» беседы) санкции. Нередко упоминается увольнение. Однако и такая, казалось бы, очевидная мера применяется лишь примерно в трети случаев. При этом чаще всего работник уходит из компании «по собственному желанию». В некоторых случаях респонденты признаются, что инсайдеры не понесли вообще никакого наказания, к ним не могут применить санкции: «В итоге — никакие... Сложно доказать вину конкретного человека».

Основных причин тому две. Во-первых, компании, особенно крупные, не склонны предавать гласности факты утечек информации и предпочитают выйти из ситуации с минимальными репутационными потерями. Вторая причина более серьёзна. Часто компании технически не могут доказать вину сотрудника и привлечь его к ответственности. Именно этим объясняется практически полное отсутствие судебных дел, связанных с инсайдерами. Серьёзная, юридически значимая доказательная база может быть собрана только с помощью специализированных технических средств контроля информационных потоков.

В подтверждение упомянутого в прошлой главе тезиса о своевременности мероприятий по защите информации можно привести мнение ещё одного

респондента: «К сожалению, никаких санкций применить мы уже не могли, так как утечка информации происходила от уволенных, либо уволившихся сотрудников. Единственное, что мы могли сделать — это дать им соответствующую рекомендацию для следующего работодателя». Пожалуй, не самая страшная санкция, если сотрудник слил информацию как раз своему новому работодателю.

Кому заниматься защитой информации

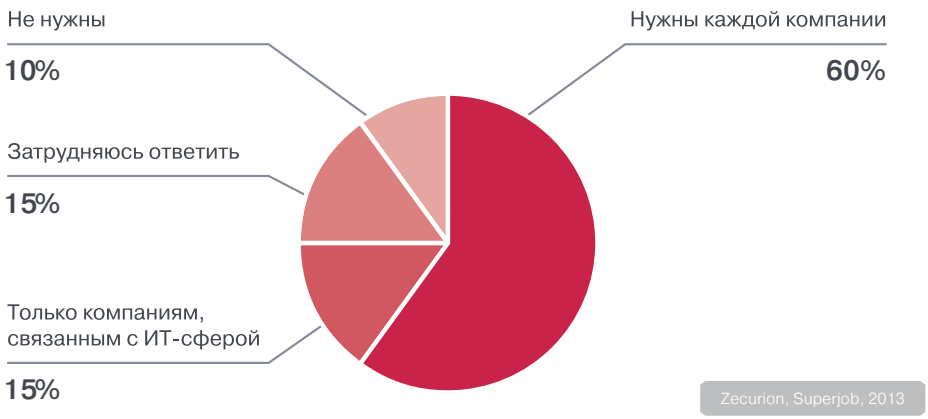
Для обеспечения надёжной защиты данных исключительно важно, кто занимается вопросами информационной безопасности в организации. Есть ли в компании выделенные специалисты (или даже отдел) или обязанности возлагаются на уже имеющихся в компании сотрудников, например, ИТ-персонал.

В попытках сэкономить и объединить несколько ролей в одном лице, руководство компаний нередко превышает допустимые информационные риски. Неприятных последствий такого объединения может быть несколько. И если с проблемой снижения производительности труда ситуацию со временем можно исправить, нанять дополнительных сотрудников, то в части информационной безопасности объединение может нанести непоправимый вред.

Универсальный специалист, например, сисадмин-безопасник сам по себе представляет серьёзную угрозу безопасности, поскольку обладает слишком широкими полномочиями. При этом часто его действия никем не контролируются. Или этого не требуется по должностным инструкциям, или вышестоящий сотрудник не обладает достаточной компетенцией для контроля специалиста, или это попросту некому делать. В результате человек с достаточно высоким уровнем доступа (знает, где какая информация хранится, кем обрабатывается, может воспользоваться учётными записями пользователей в различных электронных системах) способен нанести серьёзный урон работодателю, в том числе бесконтрольно сливать информацию, нарушать функционирование информационных систем или искажать содержимое документов. «Суперадминистратор» также способен наделить слишком большими полномочиями сотрудников бизнес-подразделений. Для минимизации подобных рисков необходимо строгое разделение полномочий и должностных обязанностей. К примеру, один человек (начальник отдела) заполняет заявку, где указывает, доступ к каким системам и программам нужен его подчинённому. Другой человек (ИТ-специалист) технически прописывает права пользователя. Третий человек (специалист по информационной безопасности) подтверждает внесённые изменения. Безусловно, такая структура несколько усложнит бизнес-процессы компании, но на безопасности скажется самым положительным образом.

В своих ответах на следующий вопрос респонденты были на редкость единодушны (см. рис. 5). Даже среди тех, кто затрудняется однозначно ответить на вопрос, немало руководителей отмечает: «Зависит от размера компании и объёма бизнеса». Положительные ответы сопровождаются достаточно категоричными комментариями. «Конечно, если фирма производит гвозди по рецептам прошлого века, то не нужен, — считает заместитель начальника правового управления из Москвы. — А если фирма конкурентоспособна — то обязательно! Однако, как и всякая защита, эта требует комплексного подхода».

Рисунок 5 ▶
Нужны ли компаниям выделенные специалисты по информационной безопасности



Только 10% руководителей заявили, что их компании не нуждаются в выделенных специалистах по информационной безопасности. Среди выбравших данный вариант ответа респондентов преобладают представители малого бизнеса. Действительно, в небольших организациях, где работает считанное число людей, большие затраты на информационную безопасность не всегда будут оправданы. К тому же тот фактор, что человек постоянно находится на виду у коллег и руководителей, снижает (но не исключает!) риски утечки данных.

Примечательно, что и в числе ответивших отрицательно, немало респондентов осознаёт необходимость защиты информации. Так, заместитель генерального директора из Москвы отмечает, что выделенный безопасник не нужен «…в конкретном данном случае, а, вообще, во всех мало-мальски насыщенных сотрудниками компаниях, считаю, нужен».

Заключение

Исследование выявило определённый дисбаланс в сфере защиты информации от утечек. С одной стороны, и руководители бизнеса, и рядовые сотрудники осознают важность информационной безопасности, понимают её цели и знают, какие данные критичны для деятельности компании. С другой стороны, на практике информация оказывается чрезвычайно уязвимой. Данные регулярно покидают корпоративный периметр и бесконтрольно используются сотрудниками на мобильных устройствах, передаются по открытым каналам связи, хранятся в незащищённых местах.

Главной причиной пренебрежения вопросами безопасности является конфликт удобства использования информации и её защищенности. Очень часто осознанный выбор делается в пользу простоты доступа к информации. Вообще, соблюдение баланса удобства и безопасности является одной из главных проблем защиты информации.

Распространённая практика удалённой работы с конфиденциальной информацией, вкупе с банальной халатностью, часто приводит к утечкам данных. Кроме того, нельзя забывать и об инсайдерах, целенаправленно сливающих информацию. Умышленные утечки могут инициировать внедрённые конкурентами, обиженные руководством сотрудники или работники, планирующие сменить место работы.

Людей не останавливают ни подписанные NDA (хотя внушительная доля компаний игнорирует даже такой элементарный способ минимизации рисков), ни грозящие за утечку санкции. Ведь реальная ответственность наступает крайне редко и часто ограничивается устным выговором или увольнением по собственному желанию. В большинстве случаев утечки вообще остаются незамеченными из-за отсутствия необходимых технических средств. По этой же причине не получается привлечь преднамеренных инсайдеров к суду — у работодателя просто нет доказательной базы.

Тем не менее, позитивным является сам факт осознания проблемы и определённые шаги, направленные на её решение. Технические средства контроля информационных потоков становятся более удобными в обращении. Можно ожидать, что с развитием законодательства в области защиты информации и ростом осведомлённости пользователей количество утечек корпоративной информации будет постепенно снижаться.

Примечательные ответы респондентов

Одна из особенностей исследования заключается в том, что каждый его участник, отвечая на вопрос, мог также оставить краткий комментарий. В некоторых случаях такие комментарии лучше всяких цифр иллюстрируют мнение респондентов. В данном разделе приведены показательные, примечательные и просто весёлые мнения, не упомянутые в тексте отчёта.

Какие санкции предусмотрены в вашей компании за разглашение конфиденциальной информации/коммерческой тайны?

— Никаких, руководство само свободно разглашает ноу-хау и технические решения, открыто водит внешних консультантов и погружает их в тонкости дел в компании. Атас…

— Голову отвернут…

Какие санкции были применены к сотрудникам, виновным в утечке корпоративной информации/разглашении коммерческой тайны?

— Отпустили с миром после внушительной беседы.

— Утечки происходили одновременно с увольнением. Нет возможности в РФ применить к сотруднику санкции в данном случае. Даже при наличии положения о неразглашении коммерческой тайны.

— Выговор/штрафные санкции, в последующем увольнение. При этом есть запрет на разглашение сумм оклада, бонусов каждого сотрудника, запрет на разглашение перестановок и планов руководства. Ужасная атмосфера в коллективе.

По Вашему мнению, какую корпоративную информацию, связанную с Вашей профессией, надо защищать?

— «Черную» кассу!

— «Крышу» нашу.

Как вы считаете, нужен ли компании специалист по информационной безопасности, который анализирует информационные риски, создаёт систему защиты информации, занимается её аудитом и мониторингом?

— Это как дважды два, те руководители, которые не понимают этого, просто не ценят труд своих подчиненных, ну, или имеют планы на «бизнес». Ко всем вопросам необходимо относиться в соответствии с масштабом проблемы, например, в ларёк нет смысла нанимать целый отдел.

— Отсутствие такого СПЕЦИАЛИСТА неизбежно приведёт к экономическим и имиджевым потерям.

— Нужен. Да и военных нужно пристраивать. Они же ничего не умеют, но кушать любят.

О портале Superjob.ru

Портал Superjob.ru (www.superjob.ru) — лидер на рынке онлайн-рекрутмента в России. Мы работаем для того, чтобы сделать жизнь в нашей стране лучше. Работа занимает большую часть нашей жизни, и если человек находится на своём месте — с удовольствием идёт на работу и с удовольствием возвращается домой — это отражается и на общей атмосфере вокруг, а мы делаем всё для того, чтобы в нашей стране таких людей стало больше! Нам это по силам, ведь количество людей, которые улыбнутся утром, потому что с удовольствием собираются на любимую работу, зависит от нас!

Наша задача — максимально удобным образом нести информацию соискателям и работодателям друг о друге. При этом мы стремимся к тому, чтобы с нашей помощью люди находили такую работу, которая давала бы им возможность расти, развиваться и получать от работы удовольствие, а работодатели — таких людей, которые максимально соответствовали бы задачам их бизнеса.

Основная деятельность Superjob.ru направлена на предоставление информационных услуг соискателям и работодателям: публикация вакансий ведущих компаний, помощь в составлении резюме, проведение тестов для соискателей, публикация статей на профильные темы, информация о тенденциях развития рынка труда. Кроме того, на портале представлен список рекрутинговых агентств, тренинговых компаний, кадровой прессы, а также анонсы кадровых мероприятий.

О компании Zecurion

ZECURION

Zecurion (www.zecurion.ru) — крупнейший российский разработчик DLP-систем для защиты от утечек информации. Компания Zecurion профессионально занимается вопросами информационной безопасности с 2001 года. В рейтинге CNews Analytics компания Zecurion уверенно удерживает первое место среди разработчиков DLP с 2011 года и входит в число 30-ти крупнейших ИТ-компаний России в сфере защиты информации. В 2012 году компания провела ребрендинг, прекратив использование старого названия SECURIT.

Линейка продуктов Zecurion реализует полный спектр защиты корпоративной информации от инсайдеров: контроль всех потенциальных каналов утечки, ведение архива действий сотрудников, защиту данных в процессе использования и хранения, реализацию и контроль исполнения политик информационной безопасности.

Комплексные системы защиты информации Zecurion на текущий момент используются более чем в 7000 организаций в России и СНГ, Европе и США, странах Азии и Тихоокеанского региона.

ZECURION
ANALYTICS

SuperJob

Контактная информация

Владимир Ульянов
Руководитель аналитического центра
Zecurion Analytics

Тел.: +7 909 691-22-12
E-mail: analytics@zecurion.com

129164, Российская Федерация, Москва,
Ракетный бульвар, 16

Тел.: +7 495 221-21-60

www.zecurion.ru

Контактная информация

Наталья Голованова
Руководитель Исследовательского центра
Портал SuperJob

Тел.: +7 495 984-77-74
E-mail: golovanova@superjob.ru

123242, Российская Федерация, Москва,
Малый Конюшковский переулок, дом 2

Тел.: + 7 495 790-72-77

www.superjob.ru