Профилактика утечек коммерческой информации

Утечка информации зачастую очень дорого обходится компании. Поэтому критически важно бороться не с последствиями, а осуществлять профилактику потенциальных утечек.

«Центр речевых технологий» предлагает комплексный подход к решению проблемы профилактики утечек на базе своих уникальных разработок в области аудиозаписи, речевой аналитики, а также голосовой биометрической верификации.

Утечка коммерческой информации – вызов времени?

Количество создаваемой в мире информации растет бешеными темпами. Разработчики систем связи постоянно демонстрируют прорывы в области обмена данными, кратно повышающих его скорость. Все это делается из благих побуждений о доступности информации каждому, кто в ней нуждается. Однако это порождает растущую угрозу для бизнеса. Ведь в информационном обществе нематериальные активы компаний приобретают особую ценность. Уникальные разработки, ноу-хау, прототипы, разрабатываемые и реализуемые решения – все это становится мишенью конкурентной разведки, промышленного шпионажа и просто недобросовестной борьбы между участниками рынка, стремящимися любыми путями достичь своих целей.

Коммерческая информация является важной, значимой и критически ценной. Подходить к ее охране стоит с не меньшей основательностью, нежели это делается для защиты материальных объектов. По этой причине важно адекватно оценивать количество потенциальных каналов утечки коммерческой информации.

Каковы факторы интенсивности утечек?

Если вы всерьез решили заняться этой проблемой в вашей компании, то вам следует обратить внимание на основные факторы, которые влияют на степень подверженности организации утечкам информации.

1. Лояльность персонала (да-да, инсайдером становятся не от хорошей жизни, лояльный персонал, как правило, соблюдает инструкции по безопасной работе с ценными данными);
2. Эффективность службы экономической безопасности при рекрутинге («вражеский агент» может быть «засланцем»);
3. Широта используемых каналов коммуникаций (чем больше способов передачи данных, тем сложнее их «обезопасить»);
4. Эффективность технических средств по защите доступа к данным (определенность и обоснованность прав доступа к данным позволяет отсечь злоумышленников на уровне рядовых сотрудников или в отдельных подразделениях);
5. Другие (существует множество факторов, однако перечисленные позволяют значительно повысить эффективность профилактики утечек).

Как обеспечить информационную безопасность предприятия?

Эффективная профилактика утечек информации строится на принципах открытой борьбы с ней, применением современных технических средств, упреждающих попытки и гарантированно доказывающих факт инсайдерской деятельности. То есть основная задача профилактики утечек – сделать так, чтобы риск обнаружения был значительно выше ценности добываемой информации.

Опыт «Центра речевых технологий» в области аудиозаписи телефонных переговоров, речевой аналитики, а также применения технологий голосовой биометрии для разграничения прав доступа позволяют решить эти задачи.

1. Проводите открытую, но сплошную аудиозапись переговоров
2. Внедрите автоматическую речевую аналитику
3. Разграничьте права доступа к информации с помощью голосовой биометрии

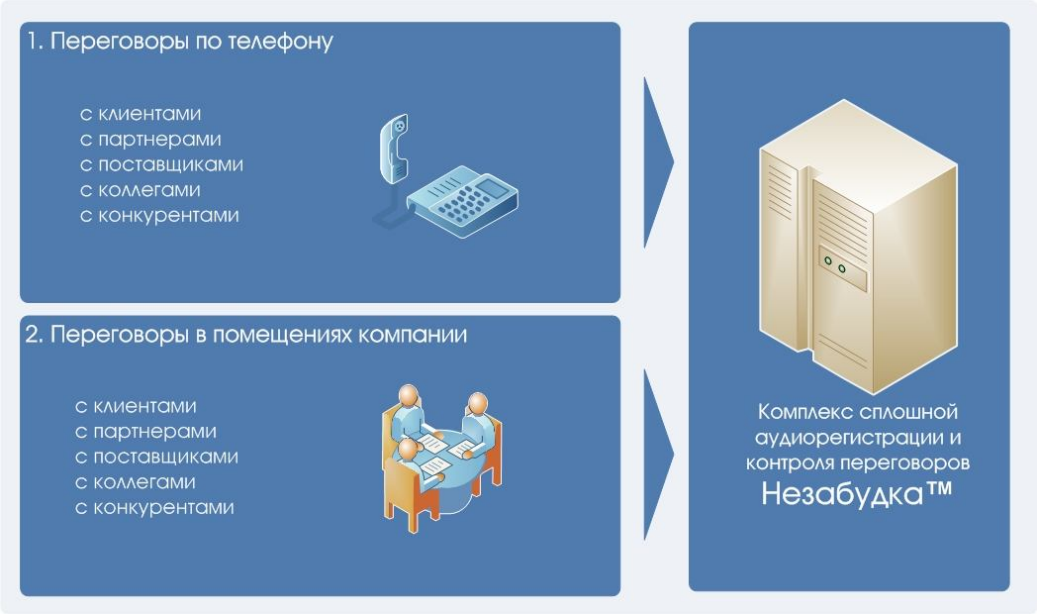
Инструмент 1: Проводите открытую, но сплошную аудиозапись переговоров

Телефонные переговоры являются неотъемлемой частью современных бизнес-коммуникаций. По этой же причине, они являются потенциальным каналом для утечек ценной информации. Наиболее мощным инструментом для его профилактики является сплошная регламентированная аудиозапись телефонных переговоров с помощью системы аудиорегистрации Незабудка™. Ведь она помнит каждое произнесенное слово.

Факт открытой аудиозаписи переговоров сам по себе является действенным стимулом для персонала к более ответственному отношению к таким процессам как взаимодействие с клиентами, партнерами, коллегами и другими контрагентами по телефону. Ведь наличие фонограмм означает наличие гипотетической возможности их прослушать, проанализировать и сделать необходимые оргвыводы. То есть, как инструмент контроля, аудиозапись переговоров являет собой весьма качественный аргумент в борьбе за эффективные и направленные на благо компании внешние и внутренние коммуникации.

С другой стороны, аудиозапись переговоров дополняет систему контроля за информацией в целом (например, DLP-системы), что значительно усложняет жизнь злоумышленникам. Сервер хранения фонограмм служит тем источником информации, на основании которой можно в дальнейшем производить ручную и автоматическую обработку, а сами записи могут в итоге оказаться материалами к делу о незаконной передаче информации. То есть работа системы не ограничивается только ролью «эффективной угрозы», но способна выступить реальным инструментом по раскрытию «дела об утечке». При этом существует возможность осуществлять запись не только телефонных переговоров, но и в комнатах для переговоров, параллельно с штатной видеозаписью. Благо, система аудиорегистрации Незабудка™ позволяет использовать

Незабудка™ позволяет осуществлять сплошной контроль переговоров >



микрофоны в качестве источников сигнала. Это позволит распространить эффект от контроля взаимодействий на личные встречи с партнерами и клиентами.

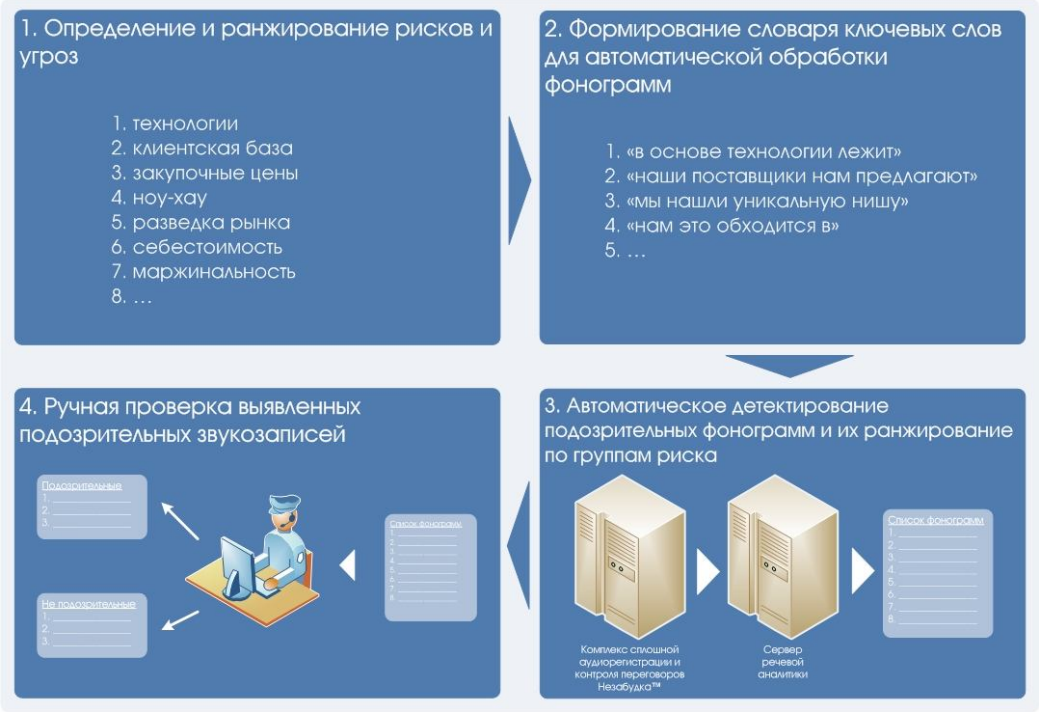
Однако важно помнить, что для использования таких систем контроля, как сплошная запись переговоров, необходимо обеспечить законность проводимых мероприятий. Для этого необходимо прописать в трудовом распорядке запрет на использование рабочих телефонов и помещений в целях, конфликтующих с интересами компании, а также указать в них, что обязательная запись переговоров является инструментом проверки этого правила. И, конечно же, ознакомить с ним сотрудников. Под подпись. Таким образом, компания осуществит легальное применение системы записи без нарушения конституционных прав персонала. А для соблюдения прав контрагентов компании необходимо оповещать их о работе системы записи переговоров перед соединением с кем-либо из сотрудников. Например, для повышения качества уровня обслуживания. Такая предварительная работа необходима для работы в рамках действующего правого поля.

Каков итоговый эффект от применения сплошной аудиозаписи переговоров? Смысл профилактики утечек заключается в том, чтобы создать ситуацию, при которой риск быть обнаруженным злоумышленником значительно превышал ценность информацию, которую он пытается раздобыть. Это действенный стимул для того, чтобы отказаться от затеянного.

Инструмент 2: Внедрите автоматическую речевую аналитику

Очевидно, что прослушать все телефонные переговоры сотрудников компании физически невозможно, крайне трудоемко и абсолютно нецелесообразно. Для этих целей более подходят более тонкие инструменты, которые способны автоматически выделять подозрительные разговоры и предлагать их для прослушивания. Этим функционалом располагает аналитический модуль системы аудиозаписи переговоров Незабудка™.

Речевая аналитика избавляет от необходимости прослушивать все фонограммы >



Инструменты автоматической речевой аналитики значительно повышают эффект от сплошной записи телефонных переговоров. Основная задача, которую они решают – определить потенциальную утечку до того, как она произошла. Для этих целей необходимо произвести достаточно сложную работу по составлению словаря ключевых слов, по которым возможно автоматическое определение разговоров, вызывающих подозрение.

Для формирования словаря ключевых слов необходима систематическая работа по определению основных угроз и рисков, выявлению мотивов, побуждающих инсайдеров сообщать секретную информацию ее покупателям. Это позволит использовать автоматические поисковые системы в профилактических целях. Например, с помощью анализа переговоров в режиме реального времени. Процесс построения словаря сводится к множеству итераций, связанных с отбором и фильтрацией слов после каждого прослушивания «ложно подозрительных» фонограмм. Однако для его развития можно использовать уже ставшие традиционными методы профилактики утечек, применяемых в технических средствах типа DLP-систем. Если в компании применяется политика классификации данных по уровню секретности, то зачастую такие файлы имеют особые имена или разряды имен, о которых знают только разработчики систем. Наличие подобных названий в фонограммах переговоров уже должны наталкивать на подозрение. И это только первый шаг к развитию системы профилактики утечек.

Эффективность речевой аналитики связана с тем, что она позволяет стандартизировать механизмы профилактики утечек на основании уже существующих данных о мотивах и моделях поведения инсайдеров. То есть, если однажды утечка уже произошла, то речевая аналитика переговоров позволит пресечь подобный способ передачи данных на основании полученной информации.

Таким образом, система профилактики утечек предприятия становится обучаемой и наращивает свою эффективность с течением времени.

Инструмент 3: Разграничьте права доступа к информации с помощью голосовой биометрии

Запись переговоров и речевая аналитика позволяют повысить риски инсайдера быть обнаруженным в случае попытки передать информацию (или назначить встречу для передачи данных). Высокий риск – хороший инструмент профилактики. Однако эффективная защита самих данных, представляющих ценность, способна предотвратить попытки передачи данных просто, потому что их невозможно украсть.

Для того чтобы обезопасить корпоративные данные, представляющие ценность для недобросовестных конкурентов и прочих злоумышленников, необходима техническая преграда в виде системы управления правами доступа к данным. Технология голосовой биометрической верификации VoiceKey™ позволяет создать эффективный барьер перед инсайдером на пути к ценной информации.

Использование голосовой биометрии в качестве инструмента верификации прав доступа к данным позволяет локализовать угрозу на уровне четко очерченного круга людей, имеющих доступ согласно должностным инструкциям. С другой стороны, биометрическая верификация позволяет точно сказать, что именно представитель группы лиц, обладающих доступом, был причиной утечки. В отличие от иных способов разграничения прав (логин-пароль, RFID-метки и другие), биометрические системы используют признаки человека и не переданных ему в пользование элементов идентификации (карточки, метки, знания).

Голосовая биометрия, в отличие других способов верификации (отпечатки пальцев, распознавание сетчатки глаз или радужной оболочки и др.), обладает двумя замечательными свойствами: верификация бесконтактна, а голосовые признаки неотчуждаемы от их владельца. Первое качество имеет ценность среди сотрудников, поскольку бесконтактные способы воспринимаются как более гигиеничные. Неотчуждаемость голосовых признаков имеет критическую значимость, поскольку даже если попытаться заставить человека пройти верификацию под угрозой, стресс отразится на голосовых признаках, и доступ не будет предоставлен. Записанный и воспроизведенный голос не пройдет процедуру верификации из-за возникающих технических искажений.

То есть в случае обнаружения факта утечки, можно достаточно однозначно определить сотрудника, допустившего ее (добровольно или непредумышленно). К тому же, использование биометрических систем верификации имеет очень сильный психологический эффект, который сам по себе способен иметь профилактическое действие на возможность утечек. В любом случае – риск слишком велик, чтобы пытаться. А не это ли самое эффективное средство профилактики?

Контакты

Санкт-Петербург

196084
ул. Красуцкого, 4
Тел. +7(812) 325-8848
Факс: +7(812) 327-9297
info@speechpro.ru

Москва

101000
Армянский пер., 7
Тел. +7(495) 623-5505
+7(495) 623-4742
+7(495) 623-3437
stc-msk@speechpro.com

Центр речевых технологий
http://speechpro.ru/