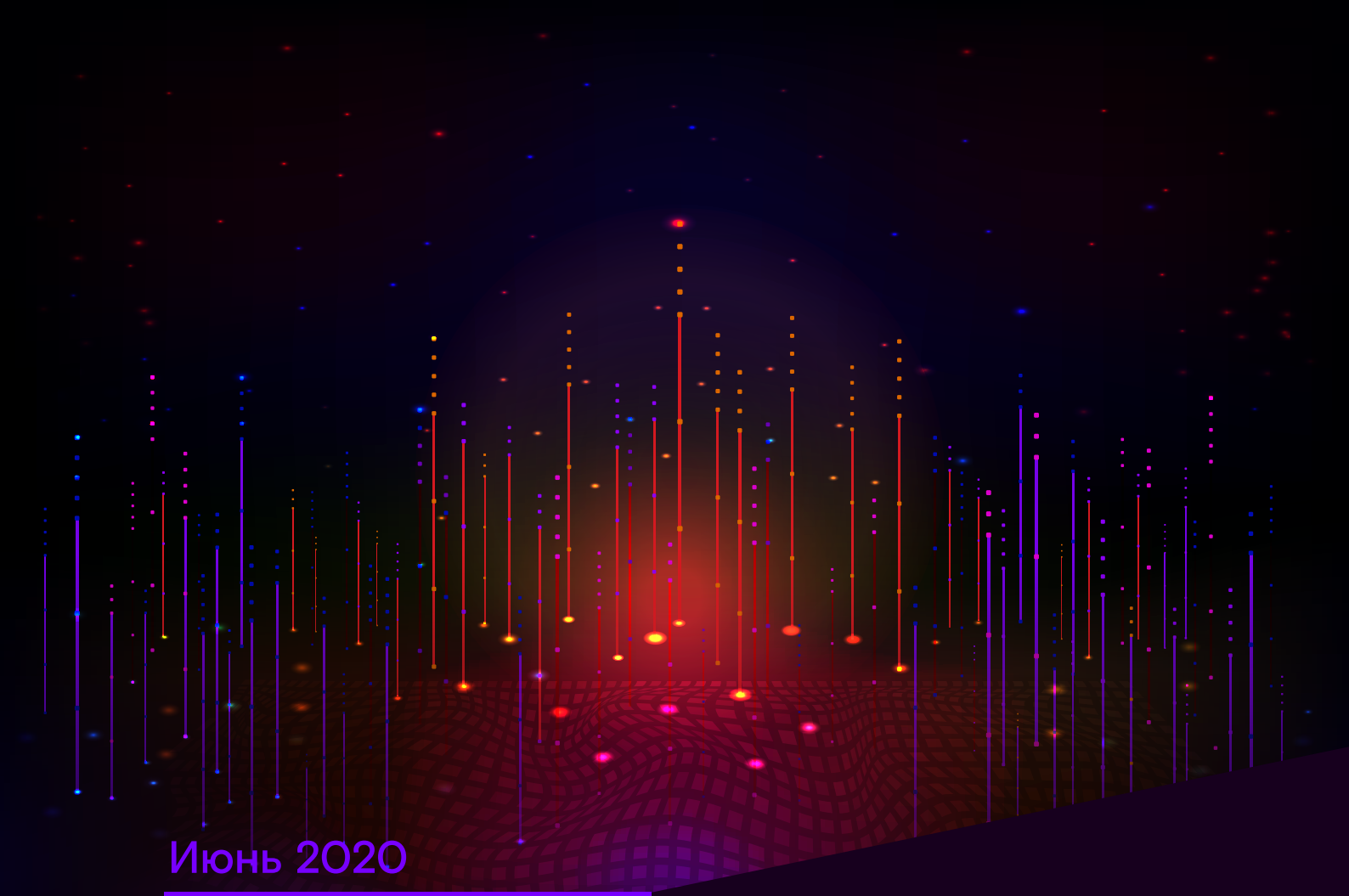


Июнь 2020

Исследование «Группы особого контроля: какие риски несут компании увольняющиеся сотрудники»

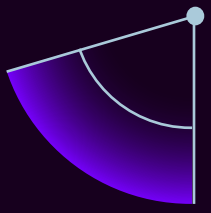
Ростелеком
Солар

Содержание

Ключевые цифры

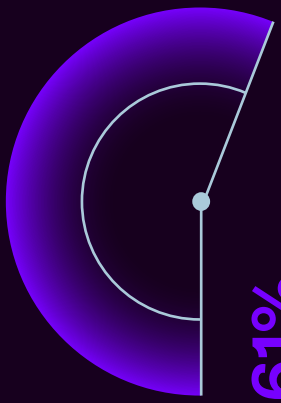
60,3%

60,3% респондентов считают увольняющихся сотрудников самой высокорисковой группой в российских компаниях.



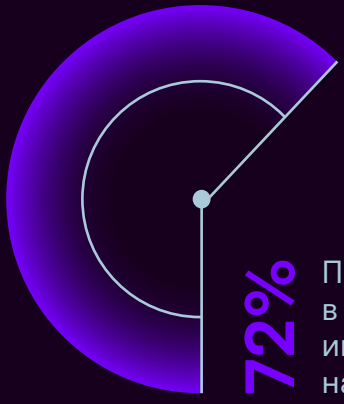
22,1%

Группа особого контроля «Участники тендерной процедуры/ключевой сделки» набрала 22,1% голосов, что вдвое превышает показатели категории «Сотрудники на испытательном сроке» (10,3%).



61%

61% участников опроса уверены, что при увольнении сотрудники выносят из компании базы данных клиентов.



72%

По мнению опрошенных, в 72% случаев унесенная информация используется на новом месте работы.

Методология

Данное исследование проведено методом электронного опроса аудитории сайта компании «Ростелеком-Солар», ресурсов нескольких популярных ИТ-СМИ, а также вебинара Solar Dozor по тематике групп особого контроля.

В опросе приняли участие представители предприятий, относящихся к сегментам Small&Middle Business, Small&Middle Enterprise и Large Enterprise.

В отраслевой ландшафт опрошенных компаний вошли сегменты ИТ/Телеком, Промышленность, Финансы, Энергетика, Ритейл, Строительство, Юриспруденция, Продажи и ряд других направлений – всего свыше 10-ти отраслей.

В процессе опроса респондентам предлагалось выбрать один из трех вариантов ответов на 5 вопросов анкеты или же указать свой вариант ответа в свободной форме.

Введение

Компания «Ростелеком-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет исследование «Группы особого контроля: какие риски несут компании увольняющиеся сотрудники».

Кризисная ситуация в российской и глобальной экономике первой половины 2020 года, вызванная пандемией коронавируса, спровоцировала такие негативные последствия для коммерческих и государственных организаций, как массовые сокращения, снижение заработной платы персонала и, соответственно, рост кадровой ротации.

Эксперты по информационной безопасности фиксируют увеличение количества инцидентов, когда увольняющиеся сотрудники пытаются вынести из компании конфиденциальную информацию с возможностью дальнейшей продажи или для использования на новом месте работы.

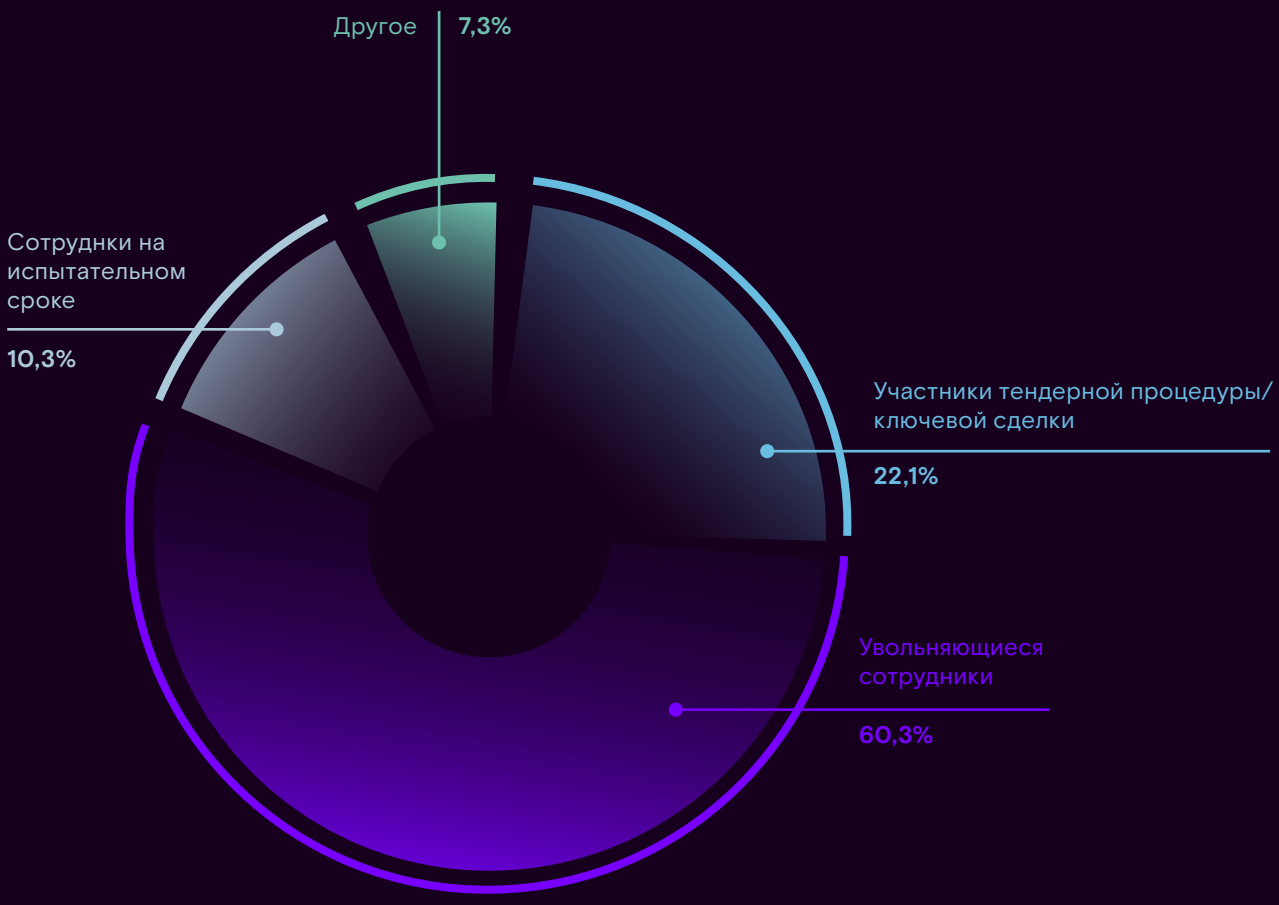
В связи с возросшей актуальностью тематики утечек данных по вине увольняющихся сотрудников аналитики «Ростелеком-Солар» решили выяснить у представителей российских компаний, считают ли они эту категорию работников основной угрозой для безопасности данных организации, какую информацию эти сотрудники чаще всего «уносят» с собой и как используют в дальнейшем.

Результаты данного исследования будут полезны как специалистам по информационной безопасности российских компаний, так и широкому кругу читателей, интересующихся тематикой утечек данных.

Результаты исследования

По результатам проведенного опроса более 60% респондентов считают основной группой риска, требующей особого внимания со стороны служб безопасности компаний, увольняющихся сотрудников. Такое же количество опрошенных полагает, что в основном покидающие компанию работники уносят с собой клиентские базы данных. А более 72% участников опроса уверены, что эта информация активно используется сотрудниками на новом рабочем месте. Ниже рассмотрим подробнее эти и некоторые другие характерные результаты опроса.

4.1 Каких сотрудников относят к группам особого контроля



Вполне ожидаемо для экспертов «Увольняющиеся сотрудники» возглавили рейтинг групп, которые представляют для компаний наивысшие риски с точки зрения утечек информации (более 60% ответов). Этот результат легко объясним с точки зрения психологии.

> Во-первых, покидающий компанию специалист стремится забрать свои наработки, либо считая их своей собственностью, либо предполагая, что они пригодятся на новом месте работы. При этом сотрудник может не иметь злого умысла навредить бывшему работодателю. Чем более ответственная должность – ближе к финансам компании (менеджеры по продажам, пресейл-консультанты и т.п.), в высокотехнологичной сфере к секретам производства, ноу-хау и разработкам (технические специалисты) и т.п. – тем лучше работник понимает, что его служебная информация является конфиденциальной. Поэтому в случае незлонамеренного выноса данных увольняющийся скорее недооценивает масштаб возможного ущерба от своих действий. В этом вопросе компаниям необходимо работать над повышением правовой культуры своих сотрудников.
>
> Во-вторых, в категории «Увольняющиеся сотрудники» всегда присутствует определенный процент людей, которые умышленно допускают утечку информации. Как правило, это обиженные на работодателя сотрудники, которые хотят его скомпрометировать, а также работники, сознательно ворующие информацию с целью дальнейшего извлечения финансовой выгоды.

Второй по популярности ответ, «Участники тендерной процедуры/ ключевой сделки» (более 22%), набрал по результатам опроса в два раза больше голосов, чем категория «Сотрудники на испытательном сроке».

По мнению экспертов «Ростелеком-Солар», это свидетельствует о том, что современные системы защиты от утечек, осуществляющие наиболее глубокий мониторинг сотрудников из групп риска, используются в компаниях не только ИБ-службами, но и другими подразделениями безопасности. Таким образом, в поле зрения безопасников попадают события, связанные с информацией по тендерам и коммуникации сотрудников по ключевым сделкам.

Ранее технологии защиты от утечек не использовались для решения задач экономической безопасности – теперь же это стало явным трендом.

Что касается категории «Сотрудники на испытательном сроке» (более 10%), здесь авторы исследования отметили явное изменение тренда. Еще 5 лет назад сотрудники на испытательном сроке вызывали у служб безопасности компаний значительно больше опасений. По мнению аналитиков, этот тренд связан с общим наращиванием компетенций корпоративными службами безопасности, а также с повышением зрелости процессов и инфраструктуры предприятий. С каждым годом растет число компаний с качественно выстроенной системой безопасности как с организационной, так и с технической точки зрения. Отлаженные процессы в таких компаниях не дают возможность новым сотрудникам получить избыточный доступ к конфиденциальной информации.

Кроме того, в последнее время значительно выросла индивидуальная ответственность линейных руководителей за сохранность конфиденциальной корпоративной информации. Не в последнюю очередь это связано с тем, что в трудовом кодексе появилась индивидуальная материальная ответственность работника за разглашение коммерческой тайны. Ведь любой инцидент с информацией, относящейся к категории коммерческой тайны, даже со стороны рядового сотрудника (неважно, новичка или старожила) всегда затрагивает и его непосредственного руководителя. Поэтому уровень ИБ-зрелости руководителей среднего звена в целом заметно вырос.

Соответственно, опасения в отношении сотрудников на испытательном сроке сохраняются либо в компаниях с недостаточно зрелыми процессами безопасности, либо на предприятиях, в отношение которых ведется конкурентная разведка.

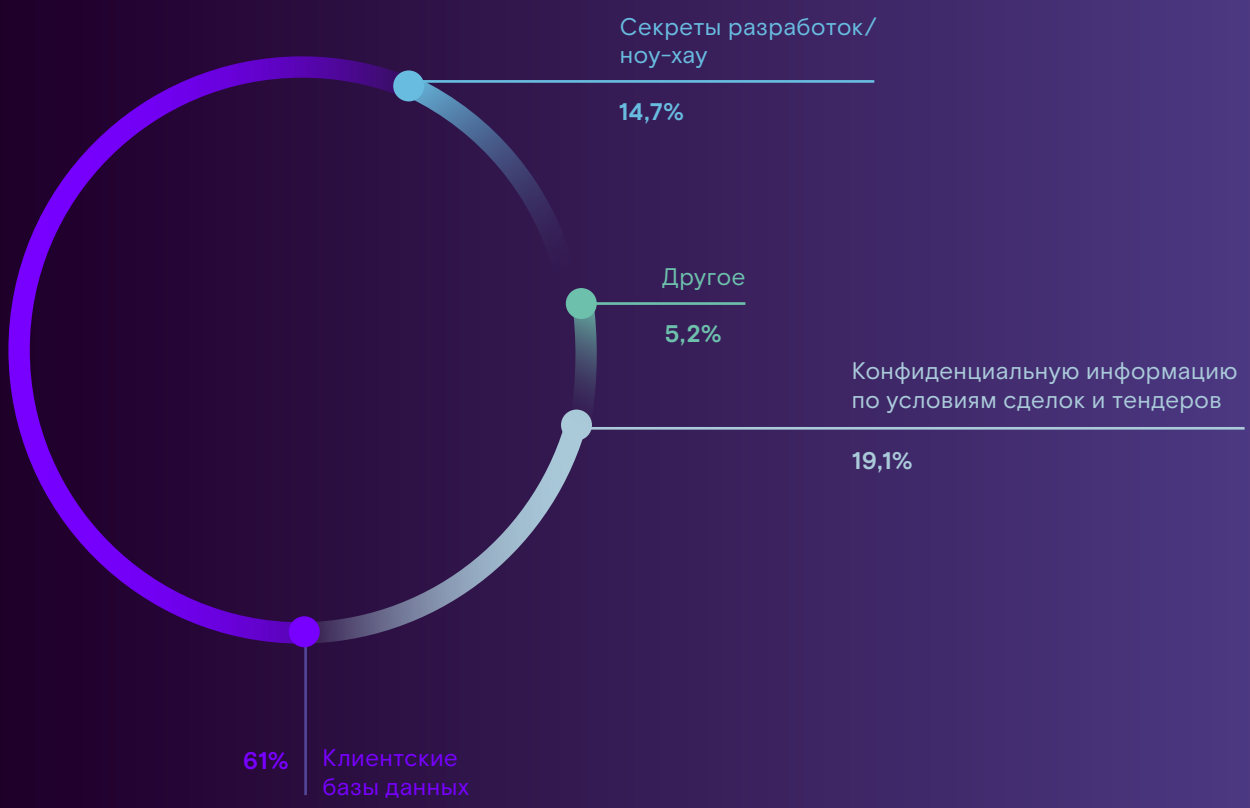
Как отмечают эксперты «Ростелеком-Солар», в условиях достаточной зрелости процессов безопасности гораздо больший ущерб компаниям с точки зрения утечек информации могут нанести давно работающие сотрудники.

Однако при этом, по наблюдениям аналитиков, именно среди сотрудников на испытательном сроке наиболее высок процент несоблюдающих требования ИБ, даже при наличии у них навыков осведомленности в вопросах защиты информации. Типичные инциденты с участием «новичков» – попытки скачивания коммерческой тайны на съемные носители и внешние облачные хранилища.

В категории «Другое» некоторые респонденты отметили такие характерные для DLP-мониторинга группы сотрудников, как «Привилегированные пользователи» (ИТ-специалисты и топ-менеджмент), «Подрядчики» и, в целом, тех, у кого есть доступ к конфиденциальной информации. При этом аналитики отмечают, что в целом приходящие в компанию сотрудники в 90% случаев просят доступ, избыточный для выполнения служебных обязанностей, мотивируя свои запросы удобством работы. И если такой доступ предоставляется, большинство сотрудников начинает нарушать требования информационной безопасности. Поэтому в целом сотрудникам достаточно доступа в информационный кластер в рамках их подразделений.

> Обобщая ответы на вопрос «Кто относится к группам особого контроля», следует отметить, что здесь актуален традиционный для DLP подход: основными объектами внимания систем защиты от утечек являются сотрудники, имеющие мотивы и/или возможность допустить утечку информации.

4.2 | Какую информацию уносят увольняющиеся



1.

Абсолютное преобладание среди ответов на этот вопрос варианта «Клиентские базы данных» (61%) закономерно – именно эти данные являются основным конфиденциальным активом любой компании. Вместе с тем, авторы исследования отмечают, что клиентская база данных – понятие достаточно широкое и имеющее отраслевую специфику. Так, в финансовой сфере клиентские базы – один из наиболее критичных активов, подлежащих строжайшей защите.

Любая внешняя встреча сотрудника в рабочее время с неизвестным лицом вызывает вопросы. Здесь DLP-системы очень активно работают в направлении контроля внешних связей. А в достаточно узкой сфере информационной безопасности клиентскую базу составляют в основном личные контакты сотрудника. И при уходе из компании специалист уносит их с собой – в таких случаях бессмысленно считать человеческие ресурсы и личные отношения конфиденциальной информацией.

61%

Кроме того, по мнению экспертов «Ростелеком-Солар», компаниям до сих пор не удается действительно надежно защитить клиентские базы от утечек.

Этот информационный актив часто хранится в организациях не только в CRM-системах с защищенным доступом, но и в виде отдельных выгрузок в различных сетевых и локальных хранилищах, в виде бэкапов баз данных и т.п. Соответственно, соотношение ценности этой информации и относительной доступности делают ее привлекательной для внутренних злоумышленников.

2.

С большим отрывом от «лидера» на втором месте по частоте упоминания расположился ответ «Конфиденциальная информация по условиям сделок и тендеров» (19,1%). Эти данные вызывают равное беспокойство с точки зрения утечек информации у представителей промышленных предприятий и сегмента ИТ/Телеком.

19,1%

3.

«Секреты разработок и ноу-хау» как объект интереса увольняющихся работников отметили 14,7% респондентов – преимущественно представители технологической сферы (ИТ/Телеком).

14,7%

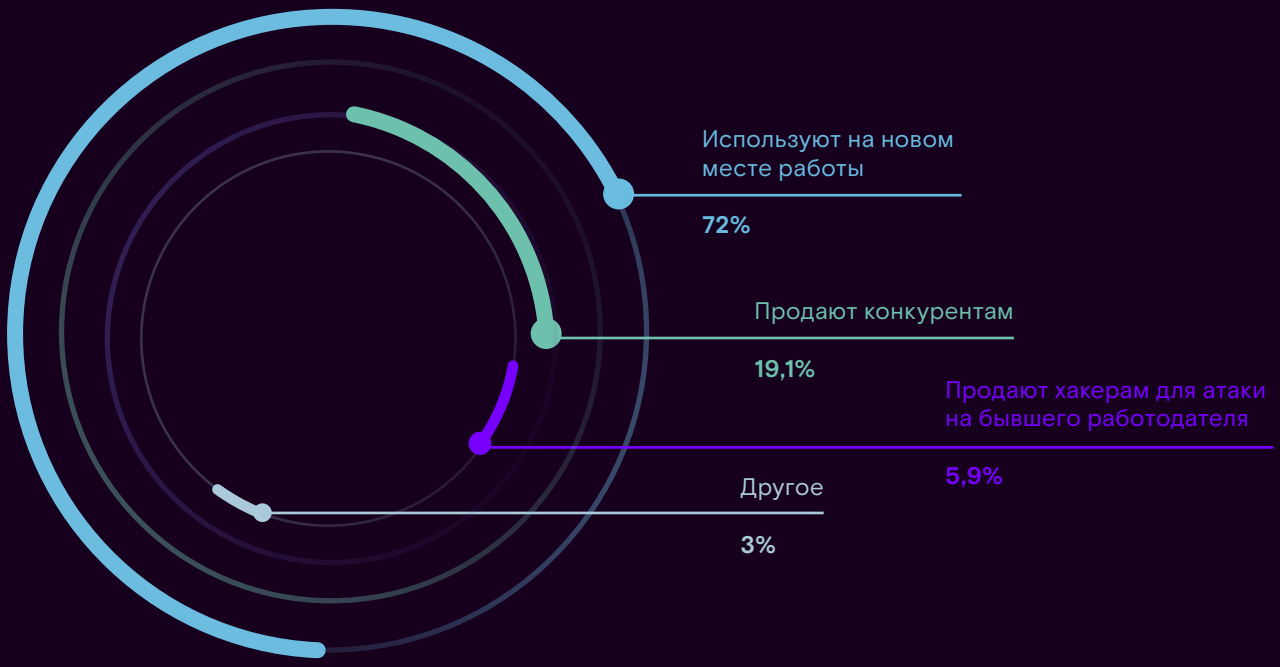
4.

По мнению авторов исследования, весьма показателен наиболее часто встречавшийся в категории «Другое» ответ «логины-пароли доступа в сеть предприятия, знание инфраструктуры». Все выбравшие этот вариант ответа респонденты отметили, что эти данные нужны увольняющимся сотрудникам для участия в подготовке целевой атаки на бывшего работодателя.

Не следует забывать о том, что для реализации успешной целевой атаки на предприятие нередко используются внутренние злоумышленники, передающие хакерам конфиденциальные данные, необходимые для проникновения в инфраструктуру. Любая целевая атака имеет следы подготовки внутри предприятия: средствами DLP можно выявить сбор информации внутри компании, нехарактерное ее перемещение и иные подозрительные активности.

5,2%

4.3 | Как используют унесенную информацию



Логичным ответом на вопрос «Как увольняющиеся сотрудники используют унесенную информацию» стала преобладающая формулировка «Используют на новом месте работы» (72%). Однако, по мнению авторов исследования, если сотрудник использует собранную информацию для сохранения собственной эффективности и ценности на рынке (один из вариантов ответа в категории «Другое»), такая утечка не несет сильного вреда компании. Если же увольняющийся сотрудник переходит на работу к прямому конкуренту и уносит у бывшего работодателя ценные наработки, которые могут дать серьезное конкурентное преимущество, например, технологическое, то это может нанести уже значительно больший ущерб.

Например, для сферы информационной безопасности характерна миграция персонала в рамках отрасли, частые переходы к партнерам или конкурентам. И лишь небольшой процент специалистов после ухода меняет направление деятельности. Поэтому, по мнению экспертов, для этой отрасли весьма актуален риск, связанный с промышленной разведкой.

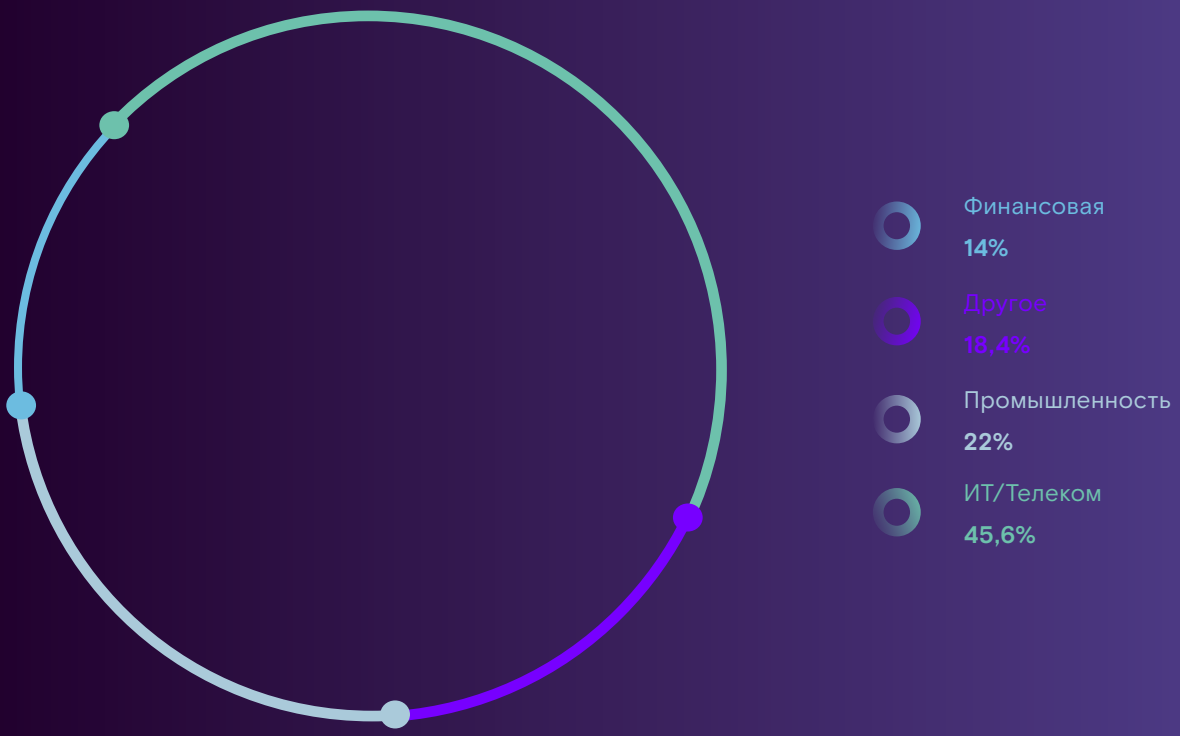
В рамках подобной инсайдерской деятельности сотрудников могут специально внедрять к конкурентам на время, с целью сбора нужной информации, а затем возвращать обратно в компанию. Или же целенаправленно искать и переманивать у конкурента специалиста, обладающего очень ценными знаниями.

Поэтому для компаний, в особенности в высокотехнологичной сфере, критичным риском является уход ключевых сотрудников.

В данном контексте высокоценными информационными активами являются различные ноу-хау и разработки компании, аналитические выкладки и результаты исследований, информация об уникальных процессах, о внутренних проблемах компании и т.п. Эти данные при эффективном применении позволят конкурентам серьезно сократить отставание или даже вырваться вперед.

В особенности этим видом риска обеспокоены представители сферы ИТ/Телеком – почти 50% всех респондентов, указавших этот вариант ответа.

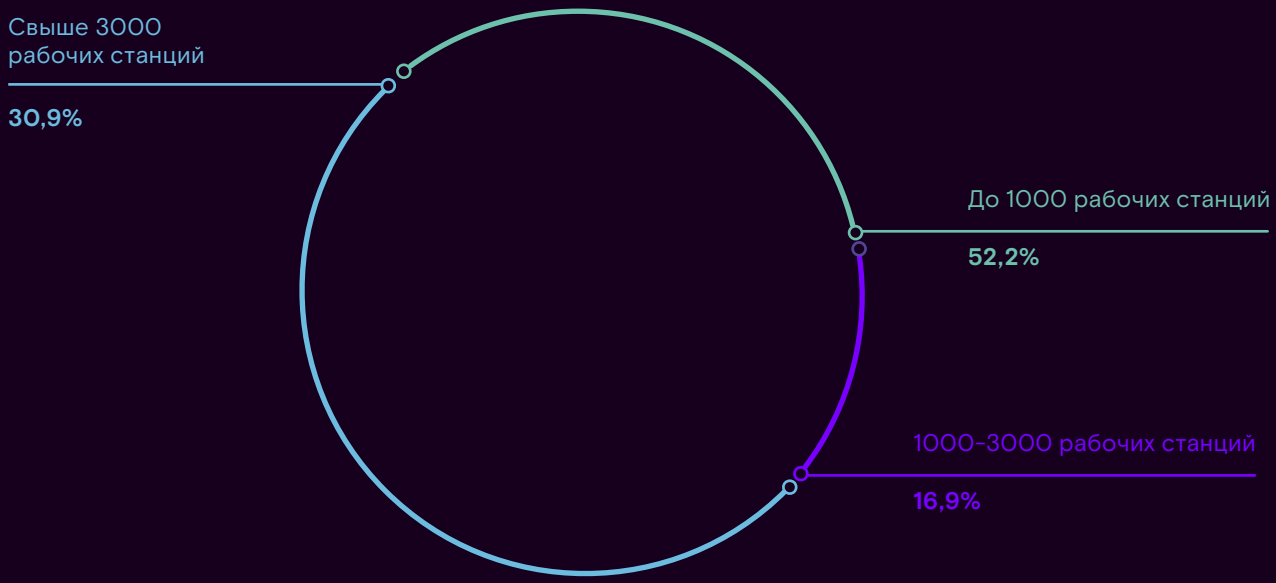
4.4 | Отраслевая специфика компаний



Результаты опроса показали в целом равномерное отраслевое распределение респондентов с некоторым преобладанием сферы ИТ/Телеком как традиционно более активной части аудитории информационных ресурсов, на которых проводился опрос.

Помимо представленных на диаграмме выше отраслей в опросе приняли участие представители сферы Энергетики, Ритейла, Строительства, Юриспруденции, Продаж и некоторых других направлений (категория «Другие»).

4.5 | Распределение опрошенных компаний по размеру бизнеса



Выводы

Результаты проведенного опроса показали, что представители российских компаний считают основной угрозой корпоративным информационным активам увольняющихся сотрудников.

По мнению большинства опрошенных, именно эта категория работников чаще всего выносит из компании клиентские базы данных, которые в дальнейшем использует, во-первых, для сохранения собственной базы знаний (ценности на рынке труда), и во вторых, для применения на новом месте работы.

Второй мотив может нанести бывшему работодателю гораздо больший ущерб, в особенности если компания ведет высокотехнологичный бизнес, для которого решающее значение имеет сохранение технологического лидерства (ИТ и Телеком, инновационное производство, научная сфера и т.п.)

info@rt-solar.ru
support@rt-solar.ru

+7 (499) 755-07-70
продажи и общие вопросы

+7 (499) 755-02-20
техническая поддержка

125009, Москва, Никитский пер., 7, стр. 1.

127015, Москва, ул. Вятская, 35/4,
БЦ «Вятка», 1-й подъезд.