Исследование инцидентов информационной безопасности, связанных с действиями увольняющихся сотрудников, 2018г.

© Аналитический центр InfoWatch. 2019 г.

Оглавление

Только цифры

2/3 случаев воздействия увольняющихся сотрудников на информационные активы работодателей связаны с копированием данных и передачей их на сторону

53% уходящих из компаний нарушителей совершали деструктивные действия в последние дни перед уходом

В **59%** утечек по вине увольняющихся сотрудников фигурирует коммерческая тайна

На долю привилегированных пользователей пришлось **27%** утечек, вызванных действиями увольняющихся

Почти **50%** утечек по вине уходящих сотрудников случились в промышленности и высокотехнологичной сфере

Аннотация

Аналитический центр компании InfoWatch представляет результаты второго ежегодного исследования инцидентов в области безопасности конфиденциальной информации, связанных с действиями увольняющихся или увольняемых сотрудников государственных организаций и коммерческих компаний.

В ходе исследования проанализированы случаи утечек конфиденциальной информации в российских и зарубежных компаниях, отраженные в сообщениях СМИ и других открытых источниках в 2018 г. и содержащиеся в базе данных InfoWatch. В каждом из отобранных для отчета сообщений были данные о деструктивных действиях увольняющихся привилегированных и непривилегированных пользователей в отношении информационных активовов работодателей.

В цифровую эпоху той или иной ценностью обладает практически любая информация, которой оперирует компания. Это и государственная тайна, и коммерческие секреты, и производственные ноу-хау, и платежные сведения, и, конечно, различные персональные данные клиентов и сотрудников. Компрометация такой информации в большинстве случаев, рано или поздно, приводит к ущербу для компании – финансовому и (или) репутационному.

Мы убеждены, что увольняющиеся и увольняемые сотрудники – особая категория риска с точки зрения безопасности конфиденциальной информации. А значит, к такой категории работников нужен особый подход для прогнозирования рискованного поведения. Покидая организацию, работники руководствуются разными мотивами. Даже те, кто не держал камень за пазухой, могут перед уходом поступить непорядочно по отношению к работодателю, приняв решение извлечь максимальную выгоду из доступных информационных активов.

> *SBS Chicago: Сотрудница окружного управления образования в Чикаго скопировала базу данных, а потом удалила ее с сервера. В хранилище были чувствительные данные более 70 тыс. человек – сотрудников, волонтеров и других лиц. Судя по всему, девушка решила украсть данные после того, как работодатель уведомил ее об увольнении.*

Результаты исследования

Сегодня одна из нетривиальных задач служб безопасности - выявление сотрудников, намеренных уволиться. Каждый из подобных сотрудников потенциально несет угрозу информационным активам. Компании важно иметь на вооружении специальную систему, способную своевременно подать сигнал об аномалиях в поведении как непривилегированных, так и привилегированных пользователей. Имея в своем арсенале подобное решение, офицер безопасности получает квалифицированную предсказательную аналитику для предупреждения инцидентов, которые могут больно ударить по бизнесу.

Классификация инцидентов предложена нами на основе той, что изложена в российском законодательстве о защите информации. Для исследования в качестве основных деструктивных действий со стороны увольняющихся сотрудников мы отобрали следующие: неправомерный доступ к информации, модифицирование и уничтожение информации, неправомерное копирование информации, неправомерное предоставление и распространение информации.

> *DigiTimes: Корейская компания Seoul Semiconductor обвинила бывших сотрудников в краже коммерческих секретов. Компания заявляет, что потратила на разработку украденной технологии производства светодиодной автомобильной оптики семь лет и более полумиллиарда долларов. По утверждению представителей Seoul Semiconductor, в результате злонамеренных действий трех бывших сотрудников эта технология оказалась доступна прямым конкурентам – тайваньской компании Everlight Electronics.*
>
> *112.ua: В Киеве разоблачен бывший сотрудник одной из финансовых компаний. За время работы он скопировал клиентскую базу, а после увольнения разместил объявление о ее продаже. В частности, за $4 тыс. он намеревался продать базу фирме-конкуренту.*

В большинстве случаев уволившийся сотрудник передает конфиденциальную информацию конкурентам компании или другим заинтересованным лицам

Как правило, нарушитель из числа увольняющихся сотрудников совершает не одно деструктивное действие. Речь можно вести об определенной комбинации. Причем чаще всего ушедший из компании злоумышленник успевает передать конфиденциальную информацию третьим лицам или воспользоваться ей ради личной выгоды (Рисунок 1).

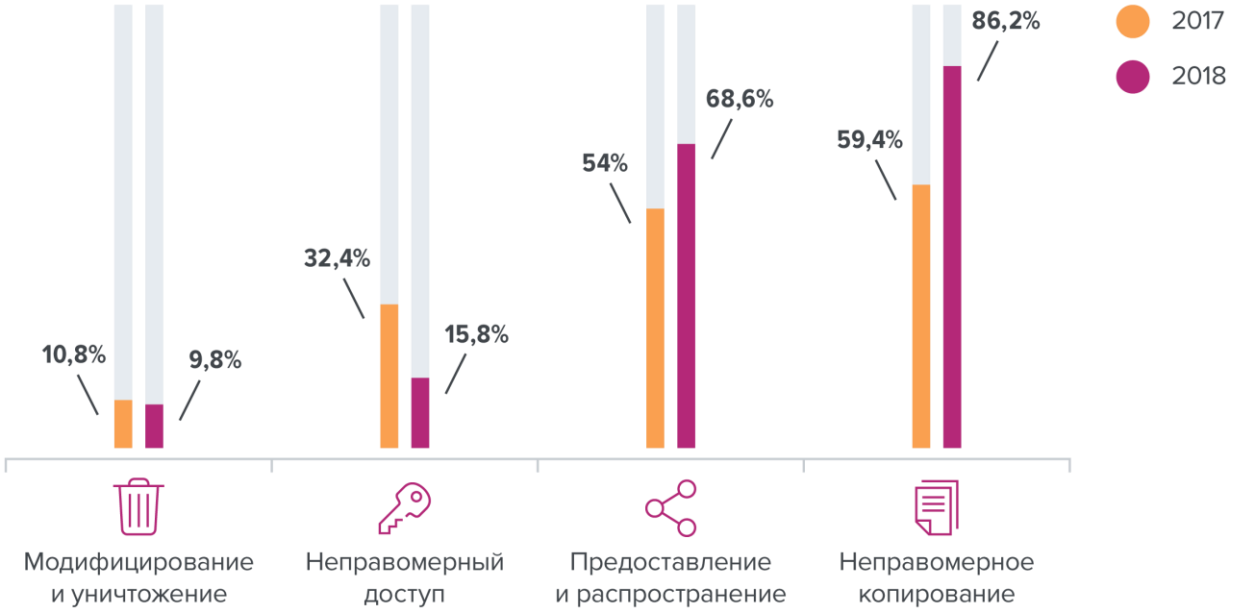

Рисунок 1. Распределение деструктивных действий увольняющихся сотрудников в отношении корпоративной информации, 2017-2018 гг.

По сравнению с 2017 г. злоумышленники из числа увольняющихся сотрудников стали существенно чаще копировать конфиденциальные данные. Примерно 2/3 всех случаев привели к передаче и распространению корпоративной информации конкурентам или другим заинтересованным лицам. В то же время в 2018 г. увольняющиеся реже проникали в хранилища информации нелегитимно и в основном использовали действительные права доступа, обращаясь к данным, которые можно быстрее всего забрать.

> *5News: Бывший сотрудник торговой сети Walmart признал себя виновным в краже данных компании и передаче их своему новому работодателю. Прежде чем уволиться из Walmart, мужчина скопировал информацию о бизнесе и тысячах товарных позиций, а затем отправил ее по электронной почте в компанию Outdoor Leisure Products, куда он перешел работать.*

В этом примере описывается типичная ситуация, когда нечистый на руку сотрудник, намеренный сменить место работы, относится к доверенной ему информации как к своей вотчине и, ничтоже сумняшеся, перед уходом копирует все, что может пригодиться ему в новой компании или при развитии собственного бизнеса.

В 2018 г. стали чаще фиксироваться случаи, когда деструктивные действия увольняющихся в отношении информационных активов приводили к прямому ущербу для работодателя (Рисунок 2). В одних случаях ущерб возникает в результате передачи

третьим лицам коммерческой тайны и производственных ноу-хау. В других к ущербу приводят мошеннические действия, связанные с необходимостью возмещения затрат пострадавшим клиентам.

> *Аргументы и Факты: В Комсомольске-на-Амуре менеджер банка перед увольнением воспользовалась персональными данными заявительницы для оформления кредитной карты на 70 тыс. рублей. Уволившись, девушка перестала платить проценты по кредиту, а претензии банка, соответственно, поступили в адрес ничего не подозревающей клиентки.*

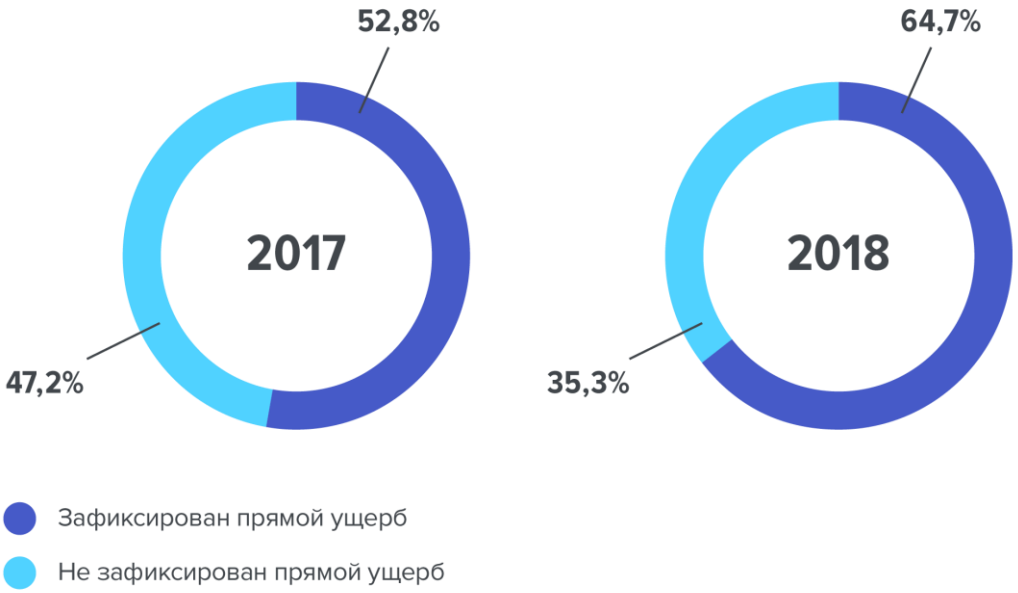

Рисунок 2. Распределение инцидентов исходя из нанесенного работодателю ущерба.

Даже если компания не фиксирует материальный ущерб в связи с действиями увольняющихся и уволенных сотрудников, почти в каждом примере можно вести речь о потере такого ценного, но трудноанализируемого актива, как репутация.

> UnGvanGuard.com: *Университет Северной Джорджии по электронной почте уведомил всех студентов о том, что уволившийся сотрудник нелегитимно обращался к их информации, защищаемой FERPA (Закон о правах на образование и конфиденциальность в семье). Экс-сотрудник мог просматривать такие данные, как имена, номера социального страхования, пол, специализация, адреса, номера телефонов, электронная почта и др.*

В половине случаев увольняющиеся сотрудники похищают данные непосредственно перед уходом.

В 2018 г. серьезно перераспределились доли по трем типичным временным сценариям нанесения ущерба корпоративным данным. Если годом ранее мы отмечали, что большинство злоумышленников начинают совершать деструктивные действия задолго, по меньшей мере за месяц до увольнения, то на этот раз первое место занял сценарий «менее недели» (Рисунок 3).

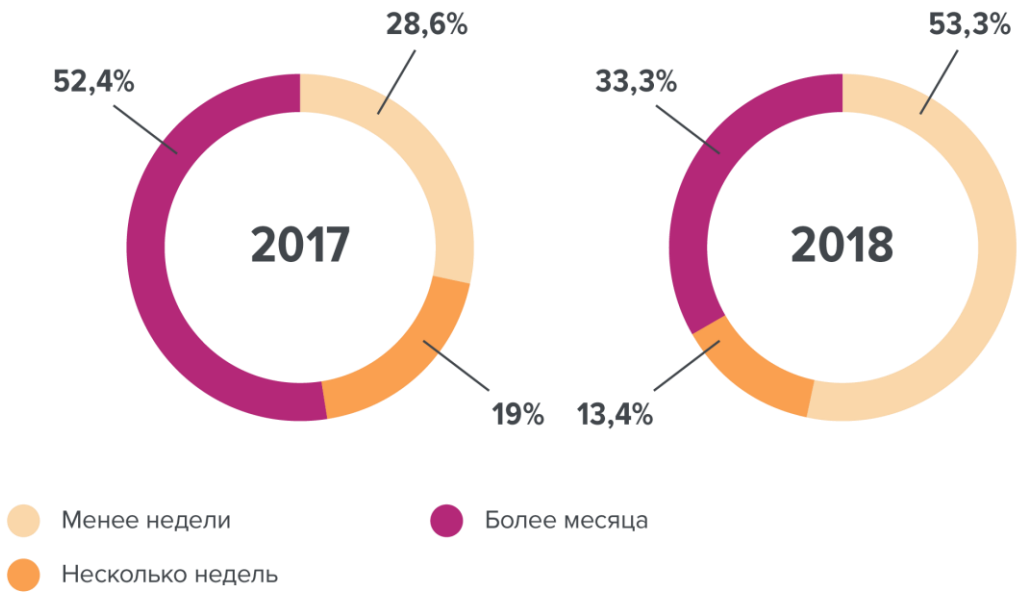

Рисунок 3. Совершение увольняющимися сотрудниками действий, повлекших ущерб. Время до увольнения.

Таким образом, в 2018 г. большинство увольняющихся нарушителей решили поживиться ценной информацией работодателя уже фактически в ходе сбора вещей, зачастую в последний день работы в компании.

К находящимся в процессе увольнения сотрудникам должно быть приковано особое внимание служб безопасности. Если контроль за информационными ресурсами ослаблен, то недобросовестный работник, распрощавшись с компанией, сможет унести множество ценной информации и причинить серьезный ущерб.

> Reuters*: Канадский авиапроизводитель Bombardier утверждает, что ряд бывших сотрудников передали японской компании Mitsubishi Heavy Industries и американскому центру испытаний AeroTEC секретную информацию по созданию и сертификации самолетов. В судебных документах уточняется, что перед уходом из Bombardier сотрудники отправили секретную документацию на личные аккаунты электронной почты.*

В 2018 г. основным информационным активом, который уносили злоумышленники из числа увольняющихся сотрудников, стала коммерческая тайна. (Рисунок 4).

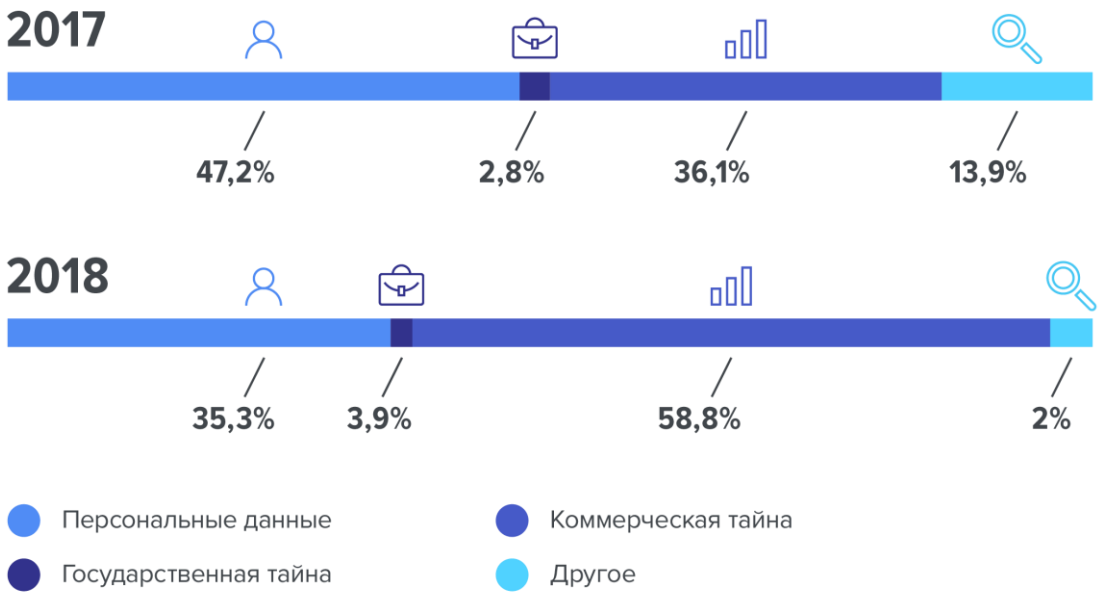

Рисунок 4. Тип данных, скомпрометированных увольняющимися сотрудниками.

> ZDNet: *Бывший инженер компании Apple Сяолан Чжан (Xiaolang Zhang) обвиняется в том, что перед увольнением похитил секретные документы, касающиеся разработки беспилотного автомобиля, и передал их своему новому работодателю – китайскому стартапу XMotors. Выяснилось, что Чжан, используя свою учетную запись, скачал порядка 40 ГБ секретной информации. Кроме того, в ходе допросов мужчина признался, что украл ряд аппаратных средств из лаборатории Apple. Однако, по его словам, сделано это было в сугубо личных интересах.*

Обострение конкурентной борьбы, гонка внедрения современных технологий и решений, самое серьезное внимание к стратегическим планам – все это приводит к тому, что коммерческие секреты и различные ноу-хау становятся критически важными данными, которые порой имеют значение государственной важности.

На наш взгляд, высокая доля коммерческой тайны в «пироге» утечек данных по вине увольняющихся во многом связана с тем, что бизнес и СМИ по всему миру стали пристальнее рассматривать случаи промышленного шпионажа, конкурентной разведки и политически мотивированных атак на интеллектуальную собственность. Одним из катализаторов всплеска интереса к защите коммерческой тайны стал

очередной виток «торговой войны» между США и Китаем. На этом фоне бизнес предпринимает дополнительные усилия по защите коммерческой информации, в том числе с использованием технических средств. В результате происходит некоторый всплеск количества зарегистрированных инцидентов, связанных с утечками коммерческих секретов и ноу-хау.

Обращая внимание читателя на сравнительно невысокую долю утечек персональных данных, необходимо сделать важную оговорку. Поскольку в поле исследования попали только утечки, нашедшие отражение в публичных информационных источниках, то, вероятно, мы имеем дело только с верхушкой «айсберга» инцидентов ИБ. Скорее всего, многочисленные случаи кражи баз данных и мошенничества с клиентской информацией остаются неучтенными как из-за привычки «не выносить сор из избы», так и из-за слабости систем защиты в отдельных компаниях, в том числе вызванной неверными настройками.

О том, что случаи компрометации корпоративных баз персональных данных приобрели масштаб эпидемии, можно судить на основе многочисленных сливов баз на хакерских форумах и в каналах мессенджеров, а также в связи с навязчивыми звонками, которые отовсюду поступают людям после обращения в банки, страховые компании, сферу услуг и т.д. Недобросовестные менеджеры, узнав персональные данные клиента, решают получить «бонус» к зарплате и сливают информацию заинтересованным лицам.

В 2018 г. более серьезную опасность стали представлять привилегированные пользователи – руководители, системные администраторы и другие категории пользователей с широкими полномочиями по работе с информационными системами и назначения прав доступа. Такая ситуация, в частности, может свидетельствовать о том, что многие компании недостаточно внимания уделяют контролю привилегированного доступа (

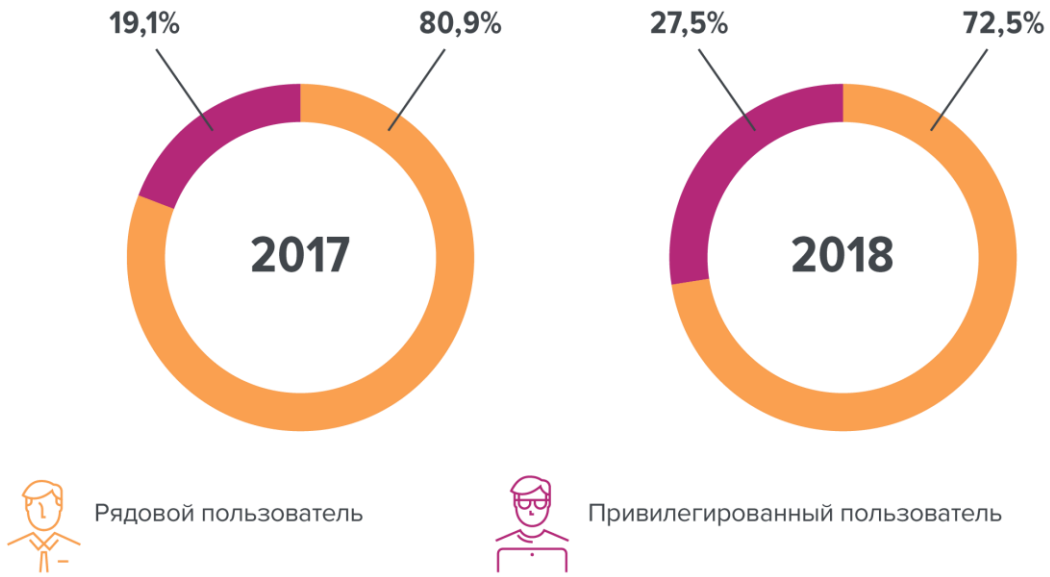

Рисунок 5).

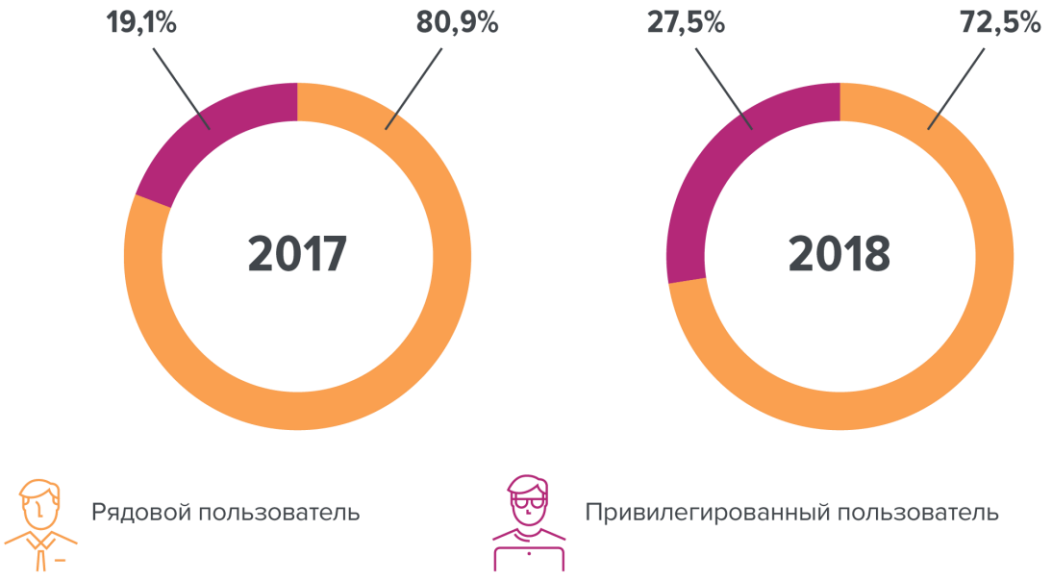

Рисунок 5. Категории нарушителей

Опасность деструктивных действий со стороны увольняющихся пользователей из числа руководителей и системных администраторов нельзя недооценивать. Функциональные роли многих руководителей предполагают доступ к массе ценной информации: финансовые отчеты, тактические мероприятия, стратегические планы, производственные ноу-хау, обширные хранилища пользовательской информации и т.д. В свою очередь, сисадмины обладают широкими возможностями управления информационными системами и назначения прав доступа. Используя свое положение со злым умыслом, привилегированные пользователи могут нанести серьезный ущерб компании. Кроме того, надо учитывать, что расширенными правами доступа все чаще наделяются подрядчики.

> CSO: *Эвард Сойбел (Edward Soibel) был техническим подрядчиком компании W.W.Grainger по обслуживанию серверов для сети вендинговых автоматов. После увольнения мужчина проник в программу управления товарными запасами и преднамеренно повредил хранящиеся в ней данные.*

На отдельных диаграммах представим мотивы, которыми руководствуются увольняющиеся нарушители из числа привилегированных (топ-менеджеры, сисадмины, часть подрядчиков) и непривилегированных пользователей. Привилегированные пользователи в 2018 г. стали гораздо чаще действовать из корысти. Покидая компании, нечестные руководители различного уровня стараются извлечь максимум ликвидной информации для комфортного старта на новом месте

работы или запуска собственного стартапа. Месть и другие некорыстные мотивы (действия под влиянием отношений, любопытство и т.д.) отошли на второй план (Рисунок 6).

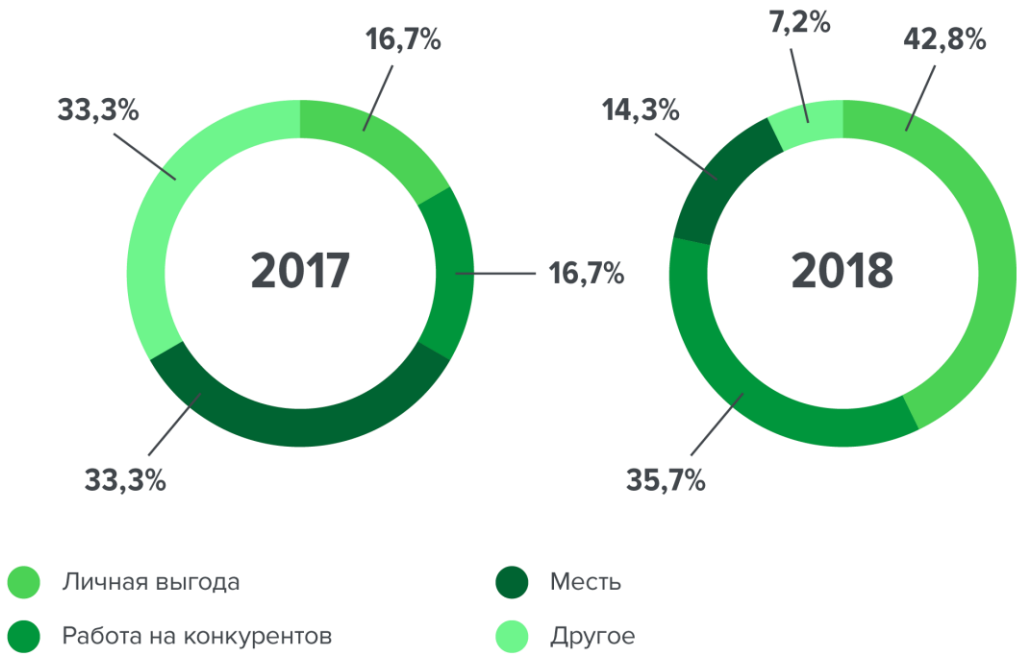

Рисунок 6. Мотивы нарушителей из числа привилегированных пользователей.

The Hindu BusinessLine: *Индийская авиакомпания-лоукостер GoAir подала в суд на своего бывшего управляющего директора Вольфганга Прок-Шауэра (Wolfgang Prock-Schauer), обвинив его в хищении конфиденциальной информации. Юристы GoAir представили в суде доказательства того, что бывший топ-менеджер похитил секретные данные перед тем, как перейти на новую работу. В феврале 2018 г. Прок-Шауэр возглавил другую индийскую авиакомпанию – IndiGo.*

В интересах конкурирующих структур стали намного чаще действовать и увольняющиеся сотрудники из рядового персонала (Рисунок 7).

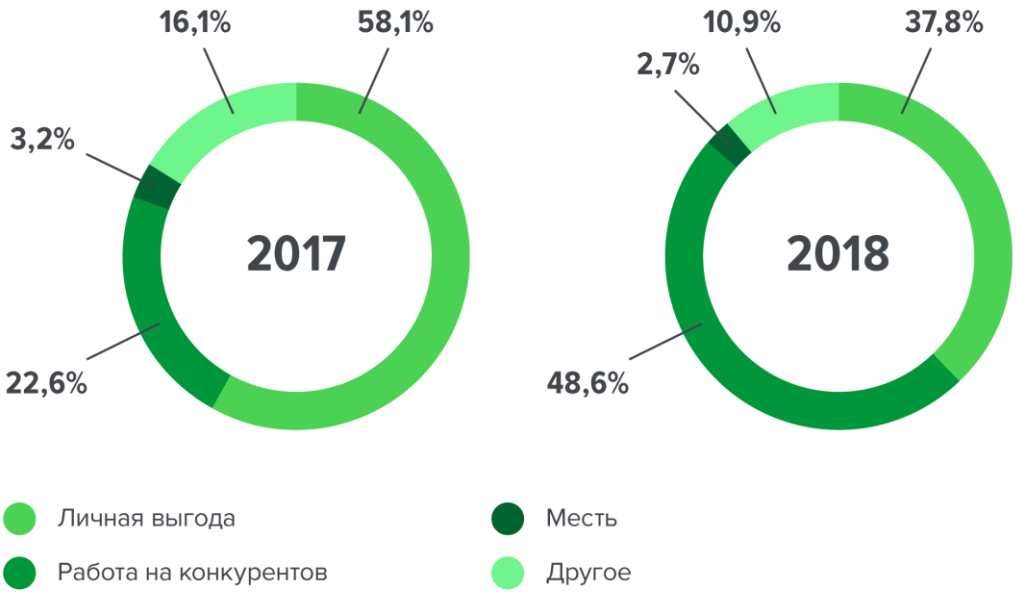

Рисунок 7

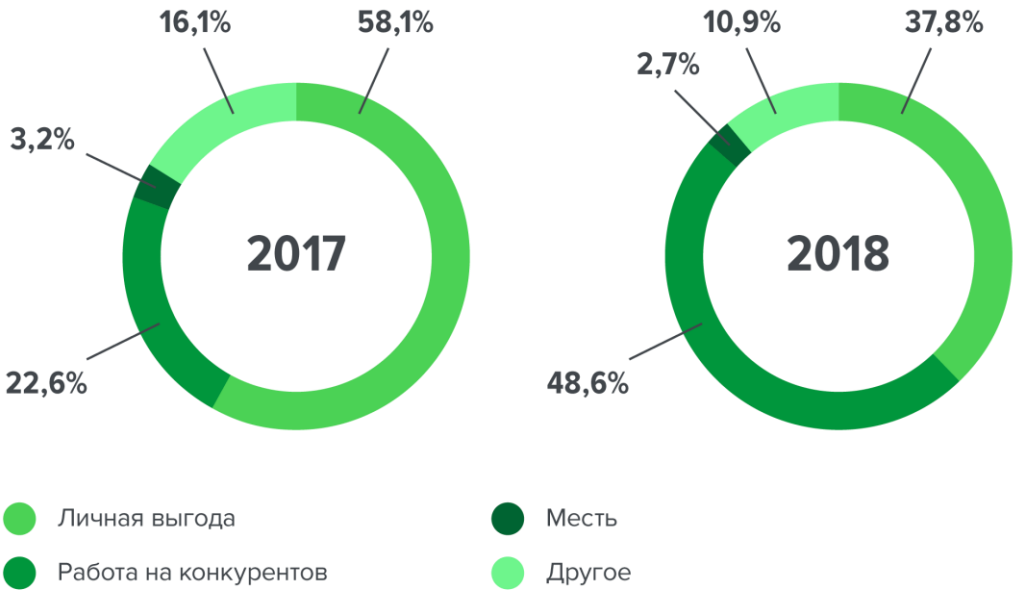

Рисунок 7. Мотивы нарушителей из числа рядовых сотрудников.

В 2018 г. серьезное перераспределение долей произошло в отраслевом разрезе. Почти в половине случаев увольняющиеся совершали деструктивные действия по отношению к информационным активам промышленных компаний и представителей высокотехнологичного сектора (Рисунок 8).

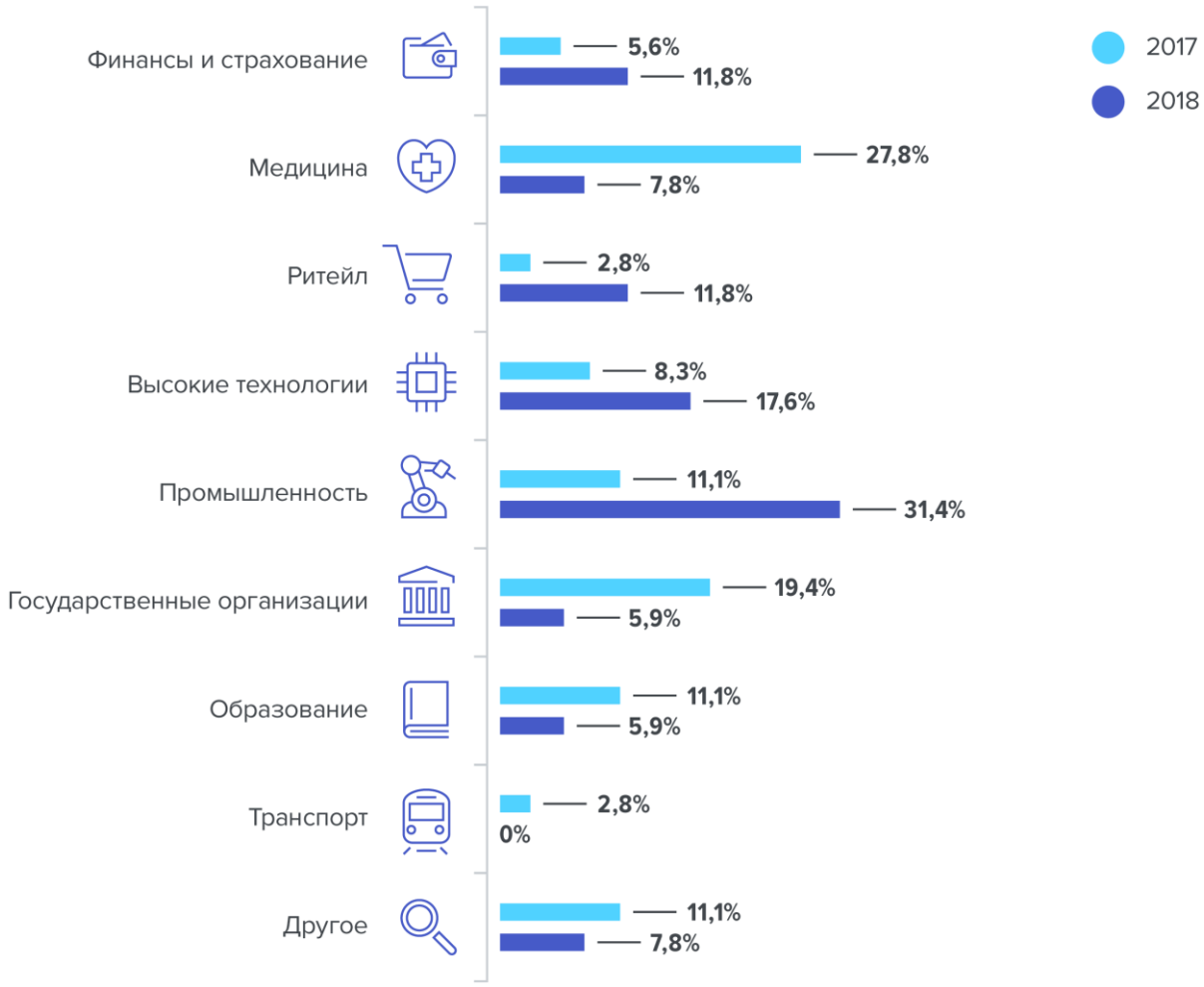

Рисунок 8. Отраслевое распределение инцидентов.

Заключение и выводы

В ходе исследования мы выяснили, что почти в 68% случаев злоумышленники из числа увольняющихся сотрудников не ограничиваются просмотром или копированием информации, а успевают передать конфиденциальные данные своих работодателей конкурентам или другим заинтересованным лицам. Каждый десятый инцидент с участием увольняющихся нарушителей связан с намеренной модификацией или уничтожением информации.

Порядка 80% рассмотренных кейсов явно указывают на корыстные мотивы нарушителей (личная выгода, работа на конкурентов). Большинство результативных действий увольняющихся в отношении информационных активов приводят к прямому ущербу, а самым ликвидным типом данных для таких злоумышленников стала коммерческая тайна.

Увольняющийся сотрудник – теоретически проблемное звено в системе корпоративной безопасности. Получив более интересное предложение о трудоустройстве, задумав открыть собственное предприятие, испытывая недовольство своим положением или уходя из компании по иным соображениям, рядовой работник или руководитель может напоследок воспользоваться доступом к конфиденциальной информации и унести с собой ценные данные. Стоит отметить, что преступный замысел может зреть задолго до самой процедуры увольнения. Поэтому так важно заблаговременно предсказать увольнение и взять на особый контроль намеренного уйти из компании человека.

Для раннего выявления угроз целесообразно воспользоваться современными решениями по прогностической (предиктивной) аналитике. С их помощью можно наладить сбор данных из множества источников, с которыми работают сотрудники, выстраивать аналитические модели и формировать профили пользователей. На основе принятых в компании регламентов, статистических моделей и возможностей машинного обучения система типа UEBA (User and Entity Behavior Analytics) профилирует отдельных пользователей, позволяет фокусироваться на однородных группах и других сущностях, вводит оценки рискового поведения пользователей на основе выявленных аномалий. В результате можно глубже понимать инсайдерские угрозы, обеспечивать более адекватное реагирование на них, принимать квалифицированные решения в области корпоративной безопасности.

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Telegram

Аналитический центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Инциденты информационной безопасности — *в данном исследовании к этой категории авторы относят случаи компрометации информации ограниченного доступа вследствие утечек данных и/или деструктивных действий сотрудников компании.*

Утечка данных — *под утечкой мы понимаем утрату контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.*

Деструктивные действия сотрудников — *действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).*

Конфиденциальная информация — *(здесь) информация, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. В данном отчете в категорию КИ мы включаем информацию, подпадающую под определение персональных данных.*

Умышленные/неумышленные утечки — *к умышленным относятся такие утечки, когда пользователь, работающий с информацией, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду. В результате создались условия для утраты контроля над информацией и/или нарушения конфиденциальности информации. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

К неумышленным относятся утечки информации, когда пользователь не предполагал наступления возможных негативных последствий своих действий и не преследовал личной выгоды. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

Вектор воздействия — *критерий классификации в отношении действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников – (Внешние атаки), направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников – (Внутренний нарушитель), атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)*

Канал передачи данных — *сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов:*

- ✓ *Кража/потеря оборудования (сервер, СХД, ноутбук, ПК), – компрометация информации в ходе обслуживания или потери оборудования.*
- ✓ *Мобильные устройства – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.*
- ✓ *Съемные носители – потеря/кража съемных носителей (CD, флеш-карты).*
- ✓ *Сеть – утечка через браузер (отправка данных в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.*
- ✓ *Электронная почта – утечка данных через корпоративную электронную почту.*
- ✓ *Бумажные документы – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации).*
- ✓ *IM – мессенджеры, сервисы мгновенных сообщений (утечка информации при передаче голосом, текстом, видео при использовании сервисов мгновенных сообщений).*
- ✓ *Не определено - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки».*