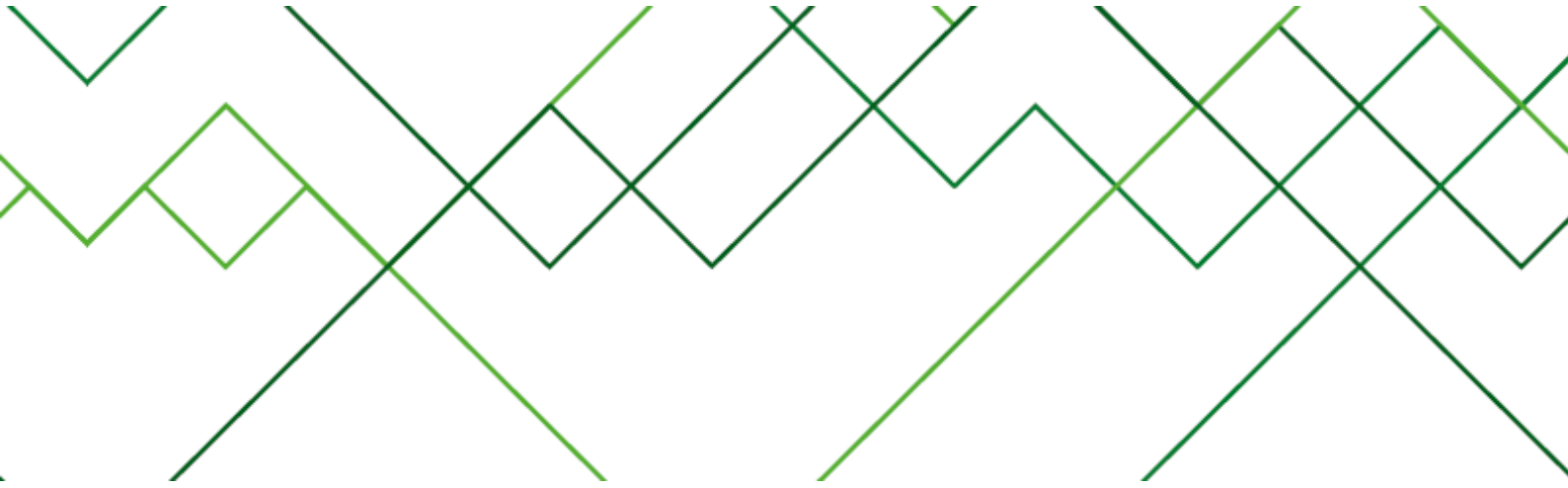
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Безопасность информации в корпоративных информационных системах. Внутренние угрозы



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Основные факты

- ✓ 77% руководителей и 85% сотрудников ИТ- и ИБ-служб считают, что опасность для бизнеса их работодателей связана не с внешними, а с внутренними угрозами.
- ✓ 73% руководителей ИТ- и ИБ-служб и более 77% сотрудников ИТ- и ИБ-служб не уверены в надежности корпоративных систем обеспечения информационной безопасности, функционирующих в их компаниях.
- ✓ 86% представителей среднего бизнеса и 75% респондентов из крупных компаний полагают, что их руководство будет охотнее инвестировать в ИБ, если доводить до него информацию о случившихся инцидентах.

Аннотация

Аналитический Центр компании InfoWatch представляет краткий отчет о первом в истории Центра практическом исследовании уровня защиты корпоративной информации[1] от внутренних угроз[2].

Мы попытались выяснить, **насколько надежно защищена информация в российских компаниях**[3], как оценивают уровень информационной безопасности (далее ИБ) компаний сами специалисты, занимающиеся защитой корпоративных данных. Какие типы внутренних угроз, с позиции специалистов, требуют повышенного внимания от ИБ-служб? Какие внутренние угрозы, прорываясь в жизнь компаний в виде ИБ-инцидентов[4], становятся причиной финансовых и репутационных потерь? Что можно сделать для повышения уровня безопасности корпоративной информации?

Огромное количество случаев, когда бизнесу был нанесен непоправимый вред, связано с действиями собственных сотрудников компаний. Хищение и продажа конфиденциальной информации[5], криминальные действия с использованием инфраструктуры работодателя, распространение информации ограниченного доступа, несанкционированные коммуникации с прессой и конкурентами, саботаж, сговоры с целью получения откатов, хищения информационных или материальных активов работодателя,– вот лишь небольшой перечень ИБ-инцидентов, напрямую связанных с внутренними угрозами.

---

[1] Корпоративная информация – здесь, информация, владельцем которой является компания.

[2] К внутренним угрозам относятся любые действия с информацией, которые могут быть инициированы сотрудниками компании или иными лицами, имеющими легитимный доступ к информационной системе, способны негативно повлиять на целостность, доступность и/или конфиденциальность информации и привести к негативным последствиям для бизнеса в виде материального или репутационного ущерба.

[3] Компании, которые основаны и/или ведут деятельность на территории Российской Федерации

[4] Инцидент информационной безопасности (ИБ-инцидент) - событие, зафиксированное системой обеспечения информационной безопасности и указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ. Реализация угрозы ИБ—нарушение свойств ИБ охраняемой информации – доступности, целостности, конфиденциальности. ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. /Стандарт ЦБ РФ СТО БР ИББС-1.0-2010.

[5] 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 исследовании в категорию конфиденциальной информации мы включаем также информацию, подпадающую под определение государственной, коммерческой, иных видов тайн.

Специалисты Аналитического Центра InfoWatch попытались выяснить, готов ли российский рынок к приходу новой эры, когда внутренние ИБ-угрозы будут безраздельно доминировать над внешними. Мы прямо спросили действующих сотрудников и руководителей ИТ- и ИБ-служб, считают ли они внутренние угрозы более опасными, чем внешние, и получили однозначный ответ – да, считают.

Это первое исследование, где представления ИТ- и ИБ- специалистов об уровне опасности[6] различных типов нарушителей[7] и типов внутренних угроз[8] сопоставляются со статистикой инцидентов.

В рамках данного исследования представлена картина реализации внутренних угроз для некоторых отраслевых вертикалей – т.е. инциденты, с которыми сталкиваются участники исследования.

Карты зафиксированных инцидентов[9] практически совпадают в пределах одной отрасли вне зависимости от размера компании. Это означает, что **средний бизнес не может чувствовать себя в меньшей опасности по сравнению с крупными компаниями**. Утечки информации, преступные действия сотрудников с использованием корпоративной информации в равной степени актуальны и для крупных, и для средних компаний.

Исследование призвано выявить и показать наиболее интересные закономерности в ограниченных (по отрасли, по размеру компаний и пр.[10]) областях объекта (внутренние угрозы корпоративной информационной безопасности).

Отталкиваясь от результатов исследования, ИТ- и ИБ-специалисты смогут по-новому взглянуть на проблему внутренних угроз – главный вызов сегодняшнего дня, - скорректировав при необходимости подход к защите информации, найти путь и

---

[6] Уровень опасности – здесь, субъективная оценка участников исследования определенного типа нарушителей и типа угроз, данная в баллах (см. Таблица 1, Таблица 2). Максимальный балл соответствует наибольшему материальному и/или репутационному ущербу, который понесет работодатель участника исследования в случае неправомерных действий нарушителя определенного типа (см. Тип нарушителя), реализации угрозы определенного типа (см. Тип угрозы).

[7] Тип нарушителя – в данном исследовании мы классифицировали субъект инцидента – нарушителя – по признаку уровня доступа к информации. Аналитический Центр InfoWatch выделяет пять типов нарушителей – Сотрудник компании, Администратор, Топ-менеджер, Подрядчик. В классификацию добавлен внешний нарушитель. Подробнее см. Глоссарий.

[8] Тип угрозы – в данном отчете мы классифицировали угрозы по признаку объекта защиты (какая информация может быть скомпрометирована в результате реализации угрозы) и по признаку особенностей действий субъекта. Аналитический Центр InfoWatch выделяет шесть типов угроз – Утечка персональных данных, Утечка платежных данных, Утечка ноу-хау, Утечка информации, составляющей коммерческую тайну, Нелояльное поведение сотрудников, Злоупотребление доступом. Классификация угроз и инцидентов совпадают. Подробнее см. Глоссарий.

[9] Карта инцидентов – диаграмма, составленная на основе данных программных продуктов InfoWatch. Карта инцидентов отражает долевое распределение инцидентов, произошедших за определенный период времени в компании, использующей программные продукты InfoWatch, зафиксированных в ходе «пилотной» или промышленной эксплуатации продуктов InfoWatch. Данные предоставлены на условиях анонимности и могут использоваться исключительно для формирования карты инцидента на уровне отрасли. В целях последующего сравнения с картами угроз, классификация инцидентов полностью соответствует классификации угроз.

[10] Принадлежность компании к вертикали, размер компании, собственную должность указывали сами участники исследования.

аргументацию для лучшего взаимодействия, прежде всего, с руководством своих компаний в целях повышения уровня защиты информации.

Методология

При проведении настоящего исследования специалистами Аналитического Центра InfoWatch применялась стандартная методология анонимного опроса, последующее сопоставление полученных данных с имеющейся фактической информацией.

Аудиторию опроса составили сотрудники и руководители ИТ- и ИБ-служб (далее участники исследования) различных компаний[11]. В течение года в рамках работы с клиентами и партнерами InfoWatch проводилось анкетирование участников исследования. Представители компаний, не являющиеся партнерами или клиентами InfoWatch, опрошены в ходе отраслевых конференций и форумов, в том числе конференции DLP-Russia'2012, DLP-Russia'2013.

Заданы следующие вопросы:

- ✓ Какие угрозы для вашей компании наиболее актуальны – внешние/внутренние?
- ✓ Уверены ли вы, что СОИБ[12] вашей компании надежно защищает корпоративную информацию от внутренних угроз?
- ✓ Считаете ли вы, что наглядная демонстрация руководству результатов работы средств защиты – выявленные или предотвращенные инциденты – способствует развитию корпоративных систем безопасности?
- ✓ Проранжируйте список нарушителей по степени потенциальной опасности для бизнеса (пять типов нарушителя). См. Таблица 1.
- ✓ Проранжируйте список внутренних угроз по степени потенциальной опасности для бизнеса (шесть типов угроз). См. Таблица 2.

Особенности заочного анкетирования с привлечением возможностей ресурса DLP-expert не позволили выдержать строгую квоту по представительству участников. В итоге авторы исследования решили строить исследование на уровне отрасли, без более детальных разрезов, тем самым преодолев ограничение, наложенное неоднородностью выборки.

В основу исследования легли представления респондентов об уровне опасности того или иного типа нарушителя, того или иного типа угрозы. Оценку типов нарушителей и угроз участники исследования дали в баллах. Максимальный балл соответствует наибольшему материальному и/или репутационному ущербу, который понесет работодатель участника

[11] В данном отчете мы различаем компании по размеру (количеству ПК) на крупные – свыше 500 ПК, и средние – от 50 до 500 ПК. Также компании различаются по принадлежности к отраслевой вертикали. Аналитический Центр InfoWatch традиционно выделяет 7 вертикалей (8-я категория – «не определено») - Банки и финансы, Медицина, Торговля и HoReCa, ИТ и телекоммуникации, Промышленность и транспорт, Госорганы и силовые структуры, Образование. От специалистов из малого бизнеса удалось получить совсем небольшое количество анкет, в связи с чем из настоящего исследования сегменты малого бизнеса и т.н. SOHO исключены.

[12] СОИБ – система обеспечения информационной безопасности – совокупность технических средств и организационных мер, направленных на защиту информации, противодействие внешним и внутренним ИБ-угрозам.

исследования в случае неправомерных действий нарушителя определенного типа (см. Тип нарушителя), реализации угрозы определенного типа (см. Тип угрозы).

Выводы исследования сделаны путем анализа результатов опроса (анкет), сопоставления карт нарушителей[13], карт угроз[14], полученных в ходе агрегирования данных опроса, с картами инцидентов[15]. Данные о количестве и типах инцидентов для построения карт инцидентов получены в процессе «пилотной» и/или коммерческой эксплуатации программных продуктов InfoWatch[16].

По результатам опроса участников исследования сформирована общеотраслевая карта нарушителей, где каждому типу нарушителя соответствует средний балл уровня опасности для бизнеса (См. Таблица 1). Эта карта сопоставляется с количественными данными об источнике (виновнике) инцидента. Классификация нарушителей при построении карт и при формировании статистических данных о реальном количестве инцидентов идентична.

Карты угроз составлены для каждой отрасли. Каждому типу угрозы соответствует средний балл уровня опасности для бизнеса (См. Таблица 2). Карты сопоставляются с отраслевыми картами инцидентов, которые также составлены на основе данных об инцидентах, произошедших в различных компаниях. Классификация угроз при построении карт и инцидентов при формировании карт инцидентов идентична.

[13] Карта нарушителей – диаграмма, сформированная на основе результатов опроса участников исследования, где каждому (из пяти) типов нарушителей присвоен определенный балл – субъективная оценка опасности для бизнеса этого типа нарушителя, данная участниками исследования. Результаты опроса сведены в таблицу (См. Таблица 1).

[14] Карта угроз – диаграмма, сформированная по итогам опроса участников исследования. Отражает представления участников опроса о том, что угрожает их компаниям. Классификация угроз совпадает с классификацией ИБ-инцидентов.

[15] Карта инцидентов – диаграмма, сформированная на основе результатов опроса участников исследования, где каждому (из шести) типов нарушителей присвоен определенный балл – субъективная оценка опасности для бизнеса того или иного типа нарушителя, данная участниками исследования.

[16] По соглашению с клиентами, мы используем эти данные без указания конкретного источника (компаний) в обобщенном (до уровня отрасли) виде.

Аудитория исследования

Исследование проводилось на случайной выборке компаний. Сотрудники Аналитического Центра InfoWatch в течение 2012-2013 гг. опросили более 918 ИБ-специалистов и сотрудников ИТ-подразделений различных компаний. В опросе приняли участие представители более 800 организаций (см. Рисунок 1)[17].

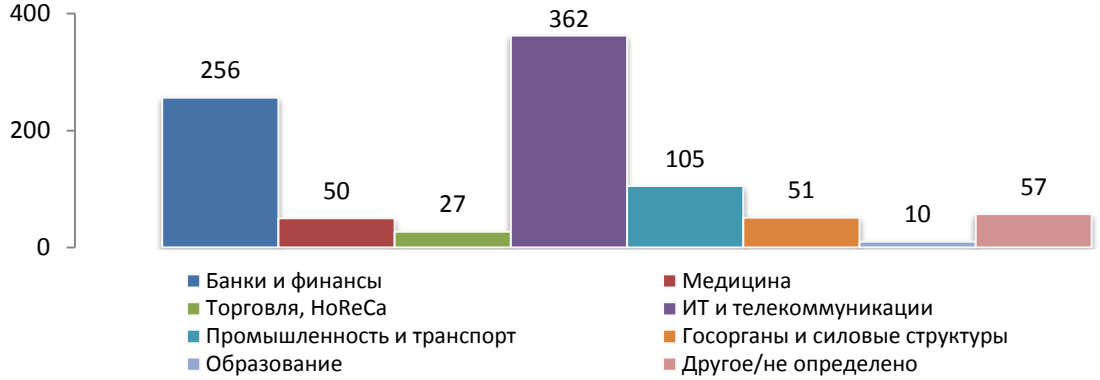


Рисунок 1. Распределение аудитории опроса по отраслям.

С точки зрения размера компаний,75% респондентов являются сотрудниками крупных компаний, 23% работают в организациях среднего размера. Специализация участников опроса: 88% составляют специалисты отделов информационной безопасности, 11% - сотрудники ИТ-служб. Относительно позиций участников: 54% руководят ИТ- или ИБ-службами. Сотрудниками ИТ- или ИБ-служб, техническими специалистами являются 40% респондентов (на диаграмме «Сотрудники» см. Рисунок 2).

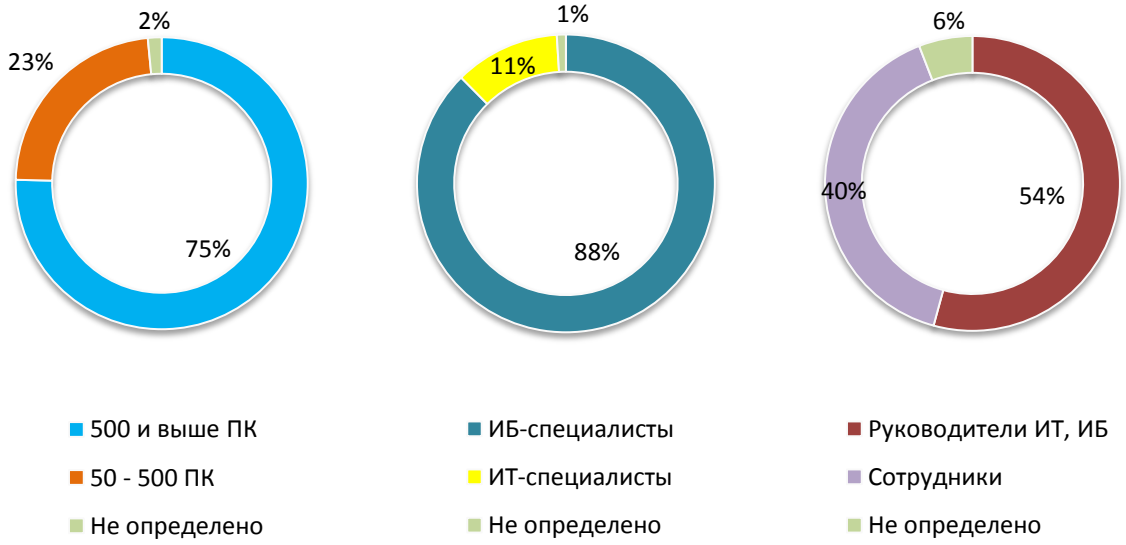


Рисунок 2. Распределение аудитории по размеру компаний (количеству ПК) и виду деятельности респондентов.

[17] В ряде случаев опрашивались несколько специалистов, представляющих одну компанию. Однако доля таких случаев составляет не более 10%.

Результаты исследования

Ключевой вывод №1. Компании считают, что основная опасность для бизнеса связана с внутренними угрозами.

В ходе опроса 77,6% руководителей ИТ- и ИБ-служб заявили, что основная опасность для бизнеса их работодателя связана с внутренними угрозами, а именно с утечкой информации ограниченного доступа, нелояльным или преступным поведением сотрудников и пр.

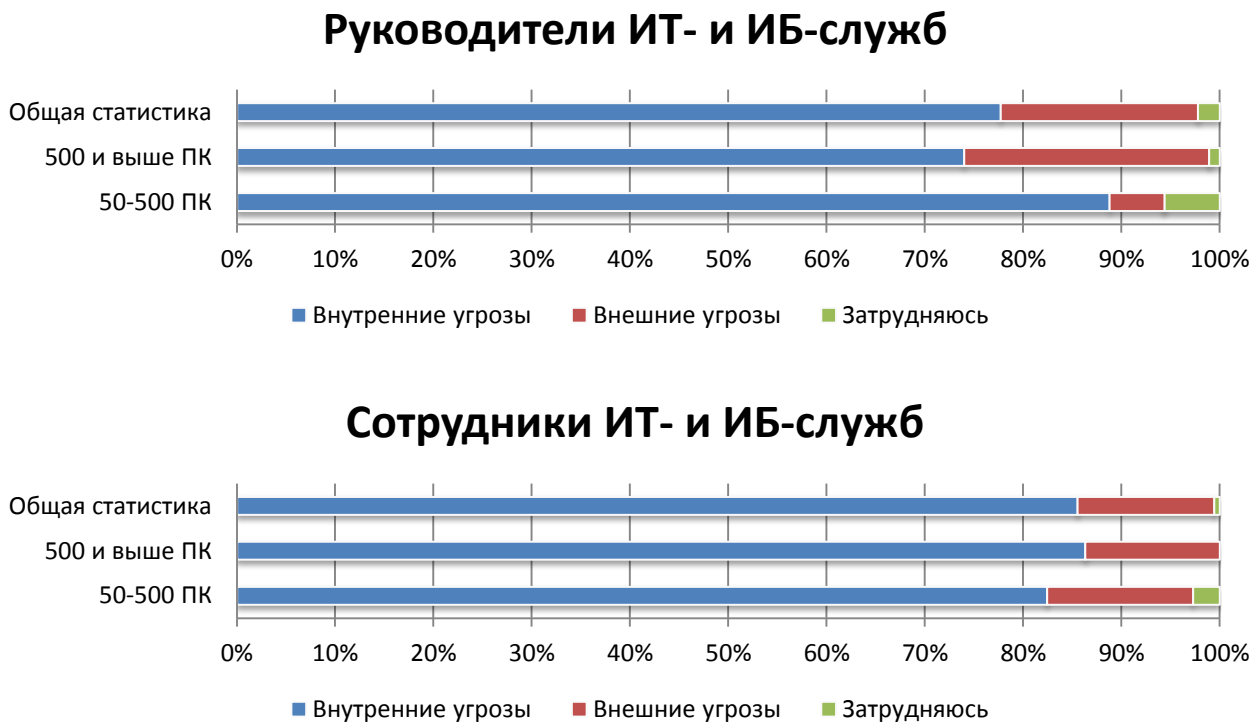


Рисунок 3. Распределение угроз по степени опасности для бизнеса.

Лишь 20,0% опрошенных руководителей считают, что б***о***льшая опасность для бизнеса исходит со стороны внешних угроз: направленные атаки, вирусы, DDoS и пр.

Процент сотрудников ИТ- и ИБ-подразделений, считающих внутренние угрозы более опасными для бизнеса, чем внешние, еще выше – 85% (см. Рисунок 3).

Столь однозначная оценка внутренних угроз как более опасных, по сравнению с внешними, не случайна. При сопоставимом уровне ущерба[18], от внутренних угроз сложнее защититься. Противодействие внутренним угрозам более затратно как с точки зрения инвестиций в технические средства защиты, так и с точки зрения дополнительных вложений в повышение квалификации персонала. От ИТ- и ИБ-служб требуется понимание того, какая информация является наиболее ценной для компании, каковы наиболее уязвимые участки в защитной системе, кто является наиболее вероятным нарушителем. Вопрос противодействия внешним

[18] Уровень возможного ущерба для бизнеса сопоставим, если понимать под объектом защиты не инфраструктуру, а информацию.

угрозам в целом менее проработан, чем защита информации или инфраструктуры от внешних угроз.

> *Если для борьбы с вирусами или другими внешними угрозами достаточно установить соответствующее ПО, то противодействие внутренним угрозам требует серьезных вложений, понимания проблематики, высокой квалификации персонала. Компании оценивают уровень опасности, связанный с внутренними угрозами, как однозначно высокий еще и потому, что конечный ущерб от внутренних угроз не всегда удается точно спрогнозировать.*

Ключевой вывод №2. Участники опроса не уверены в надежности СОИБ собственных компаний.

Сотрудники Аналитического Центра InfoWatch обнаружили, что 73,0% руководителей ИТ- и ИБ-служб и более 77,3% сотрудников этих служб не уверены в том, что система обеспечения ИБ их компаний достаточно надежно защищает информацию и бизнес организации от внутренних угроз (см. Рисунок 4).

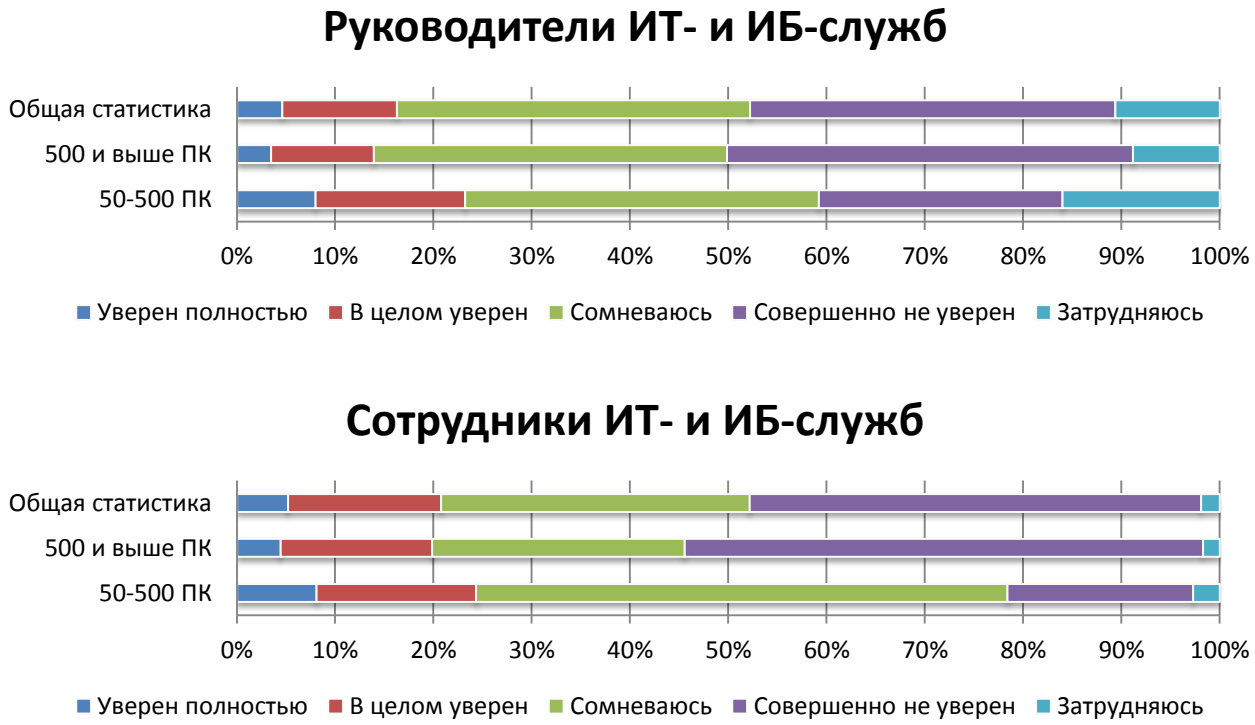


Рисунок 4. Уверенность в надежности СОИБ собственной компании.

Такое распределение можно объяснить тем, что люди, работающие в сфере ИБ, склонны, за неимением точных методик оценки уровня опасности того или иного типа угрозы, склонны его переоценивать. ИТ- и ИБ-службы постоянно ищут пробелы и просчеты в собственных системах. К тому же работы по обеспечению ИБ компаний не всегда получают достаточное для поддержания высокого уровня защиты финансирование.

Примечательно: участники исследования, считающие, что внешние угрозы более опасны, чем внутренние, заявляли о своей уверенности в СОИБ работодателя гораздо чаще, чем их коллеги, считающие, что наибольшая опасность для бизнеса исходит от внутренних угроз.

> *Участники исследования точно знают или имеют представление о том, каким образом можно повысить уровень защиты информации, улучшить системы обеспечения информационной безопасности. Большой процент участников исследования, не уверенных в собственных СОИБ, свидетельствует о недостатке финансирования ИБ-направления в отдельных компаниях, возможно, по рынку в целом.*

Ключевой вывод №3. Участники опроса неверно определяют источник наиболее опасных угроз.

В ходе исследования мы предложили участникам проранжировать список из пяти типов нарушителей (включая внешнего нарушителя) в зависимости от масштаба предполагаемого ущерба от его действий. Затем мы вывели средний балл[19] (уровень опасности) для каждого типа нарушителя.

Как видим (см. Рисунок 5), наибольшую угрозу, по мнению участников исследования, представляют сотрудники с расширенными правами доступа к информации и инфраструктуре – администраторы сети, баз данных. Само распределение, однако, получилось почти однородным – разброс результатов находится в пределах 1,7 баллов (в диапазоне 3,1- 4,8).

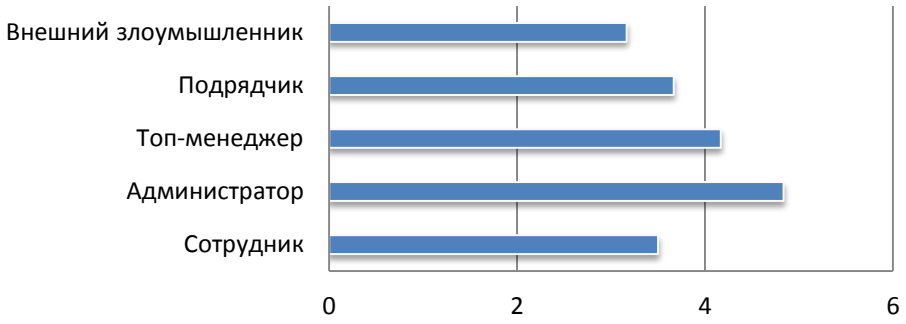


Рисунок 5. Карта нарушителей. Типы нарушителей по тяжести предполагаемых потерь для бизнеса. Средние баллы.

Сводная карта инцидентов, зафиксированных программными продуктами InfoWatch, дает иную картину. Наибольше число инцидентов связано с деятельностью совершенно определенных типов злоумышленников. Это, в первую очередь, топ-менеджмент компаний, а также подрядчики, задействованные в бизнес-процессах организации (см. Рисунок 6).

> *zdnet.com/ Пример из международной практики: бывшие высокопоставленные сотрудники AMD перед уходом в NVIDIA скопировали на флеш-диск более 100 тыс.*

[19] Средний балл = сумма баллов для данного типа нарушителя деленное на количество оценок. Подробнее см. Таблица 1.

файлов с конфиденциальной информацией, принадлежащей AMD. Инсайдеры решили покинуть AMD, прихватив с собой коммерческие секреты компании, для чего проникли на защищенные компьютеры и в течение шести месяцев собирали информацию. В числе сотрудников, обвиняемых в краже данных, упоминают Роберта Фельдштейна, бывшего вице-президента AMD по стратегическому развитию.

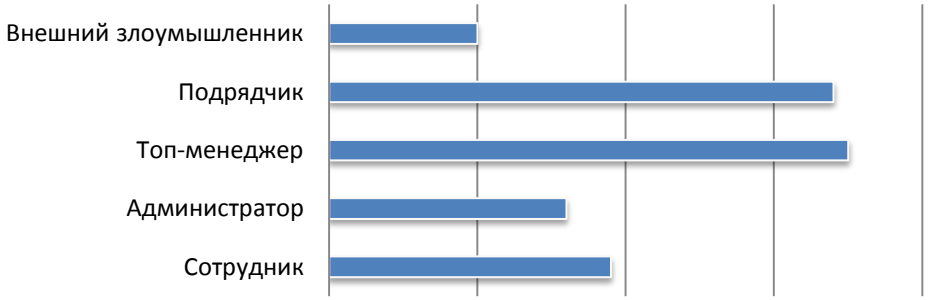


Рисунок 6. Общеотраслевая карта инцидентов. Количество инцидентов по источнику[20].

По понятным причинам, прямое сравнение двух диаграмм было бы некорректным. Первая диаграмма отражает отношение участников опроса к источникам предполагаемого ущерба для их работодателей. Вторая – количество реальных инцидентов, связанных с тем или иным источником. Оценка финансового ущерба от инцидента в рамках настоящего исследования не приводится.

Однако и без прямого сравнения заметно, что участники исследования считают равно опасными и стремятся контролировать действия всех потенциальных нарушителей, которые имеют возможность причинить вред компании. В то время как статистика указывает на применимость более сфокусированного подхода. Любой нарушитель потенциально имеет доступ к любой информации компании, потому усилия ИТ- и ИБ-служб следует смещать в сторону защиты от более распространенных типов нарушителей.

Для более эффективной защиты информации ИТ- и ИБ службам необходимо сосредоточить усилия на наиболее «опасных» направлениях, не распыляя силы по всему фронту борьбы с нарушителями.

Ключевой вывод №4. Карты угроз и инцидентов различны для разных отраслей.

Финансы и банки

Сотрудники Аналитического Центра предложили участникам исследования проранжировать (в баллах от 1 до 6) шесть типов внутренних угроз по тяжести возможного ущерба для бизнеса их компаний[21]. В своих ответах представители финансового сектора наивысшую

[20] По условиям соглашения с компаниями, предоставившими данные об инцидентах для настоящего исследования, Аналитический Центр InfoWatch не раскрывает точное число инцидентов.

[21] См. Таблица 2Таблица 2.

опасность связывают с утечкой платежных данных[22] – 5,7[23] балла. Далее по тяжести возможных последствий располагаются злоупотребление доступом – 5,1 и утечка коммерческой тайны – 4,9. (см. Рисунок 7).

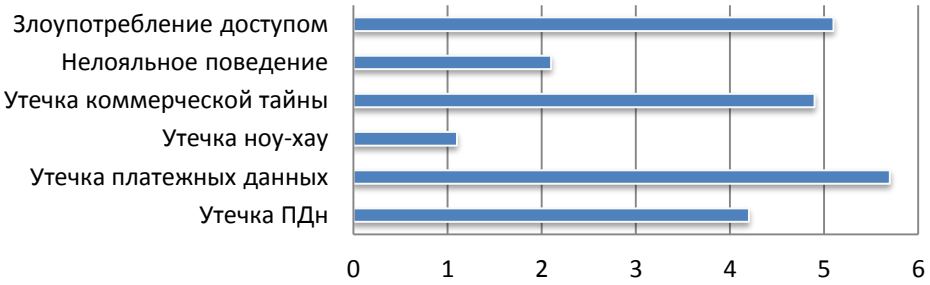


Рисунок 7. Отраслевая карта угроз по тяжести предполагаемых материальных потерь для бизнеса. Банки и финансы.

Карта инцидентов, зафиксированных программными продуктами InfoWatch в финансовых организациях, представлена ниже (см. Рисунок 8).

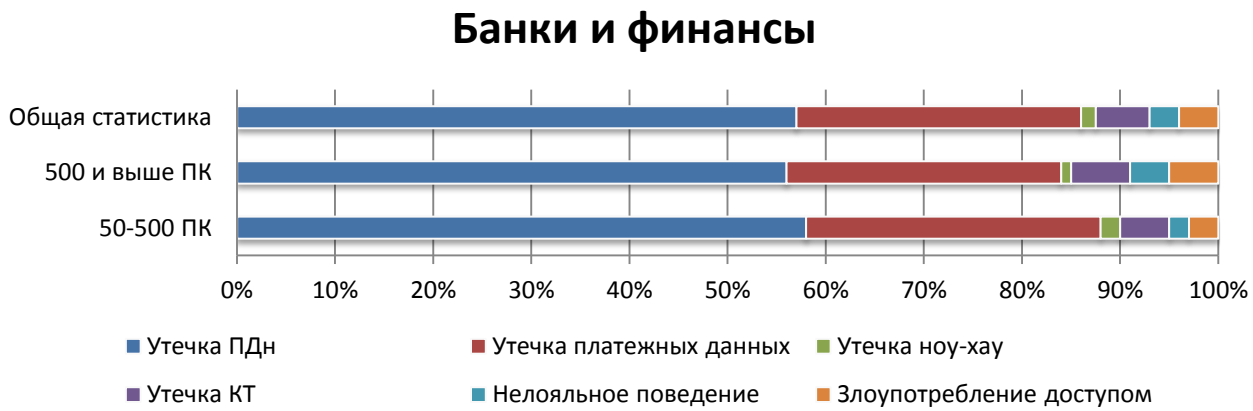


Рисунок 8. Отраслевая карта инцидентов. Банки и финансы[24].

Значительная часть случаев нарушения ИБ в финансовой сфере связана с утечкой платежных и персональных данных (более 85%).

Интересно, что потерю персональных данных менеджеры ИТ и ИБ воспринимают как меньшую угрозу, нежели утечка платежных данных, поскольку ущерб от утечки платежных данных более очевиден. Это уже не просто возможность злоупотреблений, как в случае с персональными данными, но инструмент для мошенников. Как следствие – прямой ущерб для клиентов банка, финансовые потери и репутационные издержки для банка. Однако и

[22] Платежные данные – реквизиты пластиковой карты или банковского счета. Номер и срок действия, фамилия и имя владельца, код CVC карты, кодовое слово и/или иные данные для управления банковским счетом. То есть информация, достаточная для осуществления платежа.

[23] Среднее арифметическое всех оценок, данных респондентами из финансовой отрасли.

[24] По условиям соглашения с компаниями, предоставившими данные об инцидентах для настоящего исследования, Аналитический Центр InfoWatch не раскрывает точное число инцидентов.

утечка персональных данных грозит серьезными потерями, например, если база данных клиентов оказывается в руках конкурирующего банка.

> *kazan.kp.ru/ Ленинский районный суд г. Чебоксары начал рассмотрение дела в отношении управляющего коммерческого банка. Работая с июня 2007 по январь 2010 в операционном офисе крупного банка, управляющий скопировал сведения о его вкладчиках и заемщиках, после чего уволился и устроился работать в конкурирующий банк. На новом месте он распечатал данные о клиентах с бывшего места работы и поручил подчиненным сотрудникам обзвонить их и проинформировать о наличии более выгодных условий в новом банке.*

Помимо платежных и персональных данных, в финансовом секторе «уходит» коммерческая тайна (данные о межбанковских операциях, маршруты инкассаторских автомобилей, маркетинговые планы, расчеты себестоимости банковских продуктов, стратегии развития), зарегистрированы случаи нелояльного поведения сотрудников и злоупотребления доступом к информации.

> *Сопоставление отраслевой карты угроз и отраслевой карты инцидентов показывает, что участники исследования, ранжируя угрозы, ориентируются в большей степени на последствия от реализации угроз, а не на статистику инцидентов.*
>
> *Оценка того или иного типа угрозы продиктована собственным представлением руководителей и сотрудников ИТ- и ИБ-служб о тяжести предполагаемого ущерба, характером защищаемой информации, спецификой самого бизнеса.*

Промышленность, ТЭК и транспорт

Если обратиться к картам угроз и инцидентов в промышленности, можно увидеть, что обе карты принципиально отличаются от соответствующих карт финансового сектора. В сырьевых компаниях (и ТЭК) информационная безопасность ориентирована на защиту сведений о персонале, зарплатах. Большое значение имеет защита данных о ЧП, сведений о взаимоотношениях компании с регуляторами. Потому неудивительно, что наиболее опасными угрозами представители промышленности считают утечку ноу-хау -5,7 баллов, коммерческой тайны 3,2 балла, нелояльное поведение сотрудников - 3,4 (см. Рисунок 9).

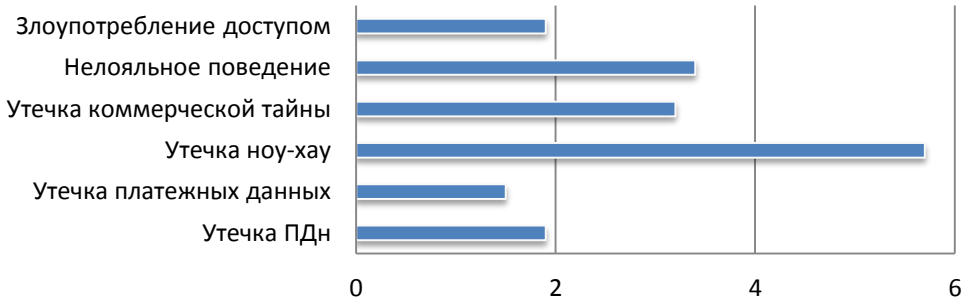


Рисунок 9. Отраслевая карта угроз по тяжести предполагаемых материальных потерь для бизнеса. Промышленность и транспорт.

Важнейшее значение для промышленных компаний имеет защита коммерческой информации – планы продаж и цены, сведения о партнерах и контрагентах, условиях сделок.

Прокуратура Вологодской обл. Обвиняемый менеджер компании, имея доступ к коммерческой информации, посредством электронной почты направлял сведения о ценах на продукцию ОАО «С» для ряда ключевых клиентов руководству ОАО «М» (г. Москва). Используя свой персональный компьютер на рабочем месте, он по электронной почте отправил интересующие сведения в обмен на вознаграждение в 250 тыс. рублей.

Показательна ситуация с защитой специфической информации в ТЭК. К такой информации можно отнести данные о недрах, геологических изысканиях, разведанных месторождениях, произошедших чрезвычайных происшествиях, их масштабе и проч. – коммерческая тайна в нашей классификации инцидентов (см. Рисунок 10).

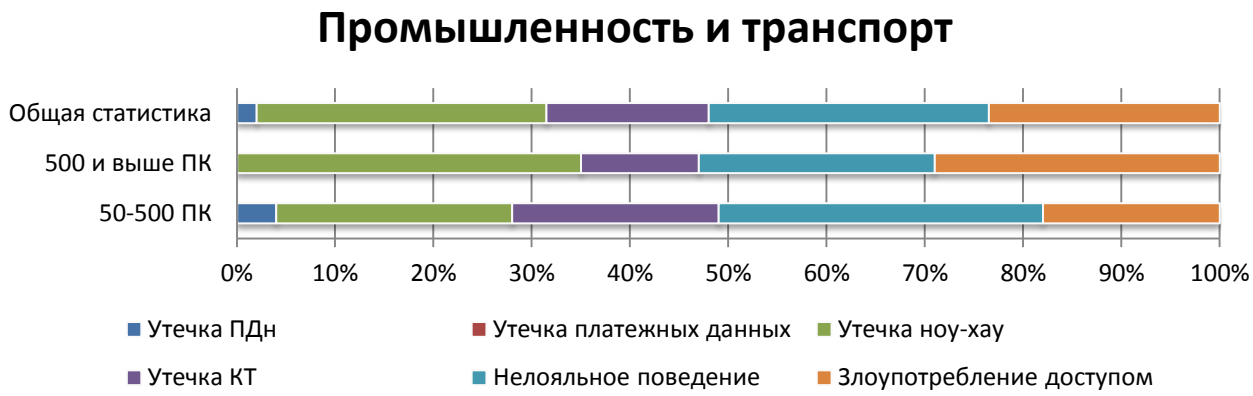


Рисунок 10. Отраслевая карта инцидентов. Промышленность и транспорт.

Наиболее «ликвидной», то есть востребованной конкурентами, является именно коммерческая тайна, поскольку ее утечка может сыграть на руку конкурентам или прямо повредить компании в случае обнародования в СМИ.

ИТ- и телекоммуникационные компании

Участники исследования из ИТ и телекоммуникационных компаний считают, что высший приоритет по степени возможной опасности для бизнеса принадлежит утечкам ноу-хау – 5,6 баллов, далее следуют утечка платежных данных – 4,8 балла, утечка коммерческой тайны – 4,7. (см. Рисунок 11).

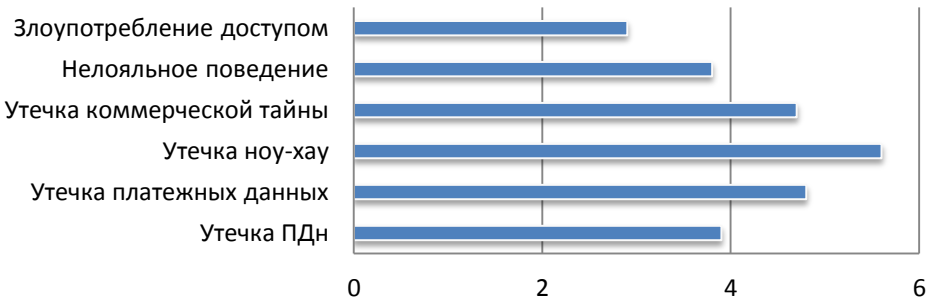


Рисунок 11. Отраслевая карта угроз по степени предполагаемых материальных потерь для бизнеса. ИТ и телекоммуникации.

Отраслевая карта (см. Рисунок 12) показывает, что доля инцидентов этого типа в общем распределении невелика – большая часть инцидентов связана с утечкой персональных данных.

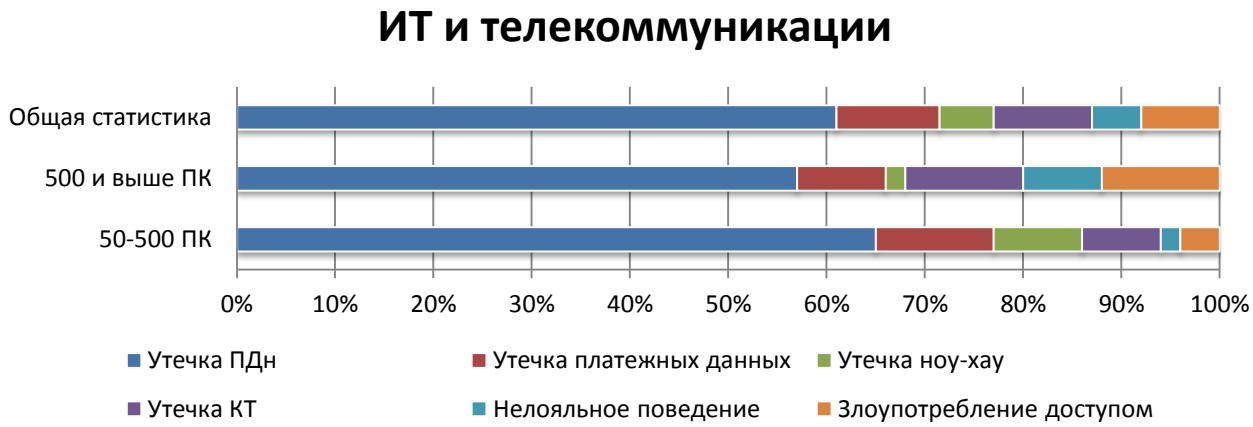


Рисунок 12. Отраслевая карта инцидентов. ИТ и телекоммуникации.

После громкой утечки SMS-сообщений в компании «Мегафон», операторы связи всерьез озаботились защитой конфиденциальных данных и переписки клиентов. Проводится большая работа по предотвращению мошенничества в сетях операторов. Однако и федеральные, и региональные операторы связи пока не преуспели в деле борьбы с хищением и распространением персональных данных абонентов. Базы данных абонентов любого сотового оператора по-прежнему можно приобрести на рынках и в интернете.

> *rosbalt.ru/ Стажер одного из телеком-провайдеров скопировал базу данных контрагентов, информацию о заключенных договорах и алгоритме производственного процесса. Разослал по электронной почте сообщения прямым конкурентам фирмы с предложением приобрести у него эти сведения. При передаче 50 тысяч рублей за продажу данных на диске мужчину задержали.*

Относительно низкая (3,9) оценка угрозы утечки персональных данных связана с тем, что операторы сотовой связи, провайдеры и прочие игроки телеком-рынка фактически закрывают глаза на неконтролируемое распространение сведений об абонентах, неправомерное использование персональных данных и номеров телефонов (в том числе в целях мобильного мошенничества). Прямой ущерб от утечки персональных данных для самих операторов довольно незначителен (небольшие штрафы), а сам факт утечки не является достаточной причиной для оттока абонентов.

> *Приведенные отраслевые карты угроз совершенно различны. Также отличаются друг от друга отраслевые карты инцидентов. Это означает, что ИБ как сфера все дальше уходит в отраслевую специфику. Что неудивительно – ценность информации определенного типа неодинакова для различных отраслей. ИТ- и ИБ-специалисты научились фокусировать доступные силы и средства в борьбе с внутренними угрозами, опираясь на представление о ценности информации в своей отрасли.*

Ключевой вывод №5. На формирование картины ИБ-инцидентов в организации больше влияет отраслевая принадлежность, чем размер компании.

Некоторые участники нашего исследования, использующие программные продукты InfoWatch, любезно согласились поделиться статистикой зафиксированных инцидентов[25]. На основе этой информации мы составили карту инцидентов по четырем отраслям, чьи представители приняли наиболее активное участие в исследовании. Три отраслевые карты инцидентов приведены в предыдущем разделе (см. Рисунок 8, Рисунок 10, Рисунок 12), ниже – карта инцидентов в госорганах и силовых структурах (см. Рисунок 13).

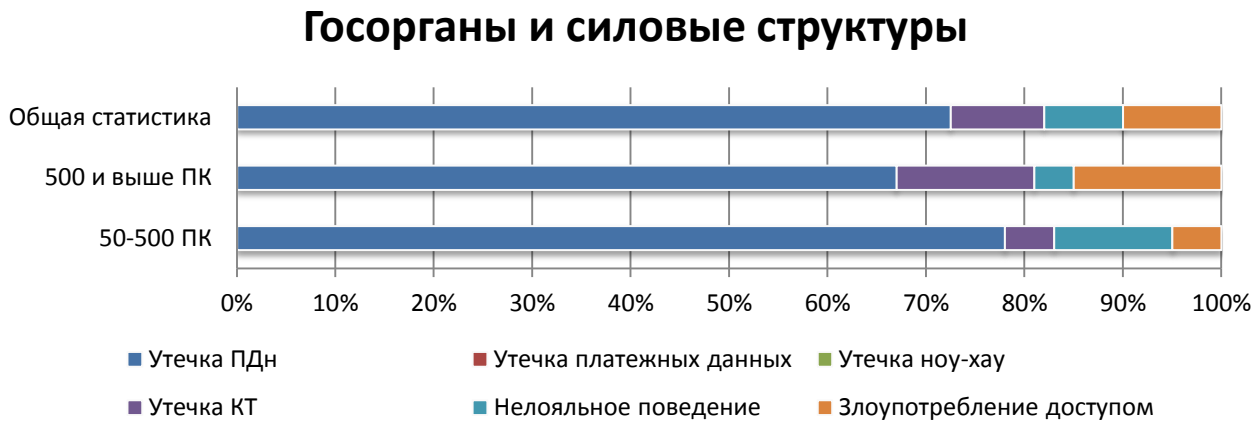


Рисунок 13. Отраслевая карта инцидентов. Госорганы и силовые структуры.

Если для банков и финансовых организаций основным типом инцидента (более 80%) является утечка персональных данных и платежной информации, то в промышленности мы видим явное преобладание трех типов инцидентов – утечка ноу-хау, нелояльное поведение сотрудников (сговоры с целью получения отката, шпионаж, саботаж) и злоупотребление доступом (нелегитимное получение доступа или хранение охраняемой информации). В ИТ- и телекоммуникационных компаниях львиная доля инцидентов связана с утечкой персональных данных. Платежная информация, по сравнению с банками, уходит реже. Наконец, госорганы и силовые структуры более всего страдают от утечек персональных данных, большая доля инцидентов приходится на утечку коммерческой тайны – сведений о тендерах, условиях сотрудничества.

> *Отметим принципиальную схожесть карт инцидентов в больших и средних компаниях в рамках одной отрасли. Это означает, что среднему бизнесу для успешного противодействия внутренним угрозам необходимо приложить не меньше усилий, чем крупным компаниям. Противодействие внешним угрозам, напомним, требует от среднего бизнеса гораздо меньше усилий, поскольку спектр угроз в среднем бизнесе уже, интерес злоумышленников к среднему бизнесу не столь высок, как к крупным компаниям.*

[25] Компания InfoWatch и Аналитический Центр InfoWatch не имеют доступа к статистике ИБ-инцидентов, фиксируемых программными продуктами InfoWatch, кроме как по прямому запросу и с согласия клиентов InfoWatch.

Ключевой вывод №6. Драйвером развития СОИБ в среднем бизнесе остается инцидент.

Участники опроса подтвердили, что наглядная презентация результатов работы средств защиты информации является одним из необходимых условий для развития систем информационной безопасности в компании. Имея на руках подтвержденные факты неправомерных действий сотрудников, утечек информации ограниченного доступа, сотрудникам и главам ИТ- и ИБ-служб проще достичь взаимопонимания с руководством бизнеса, добиться увеличения бюджетов на информационную безопасность, расширения собственных полномочий.

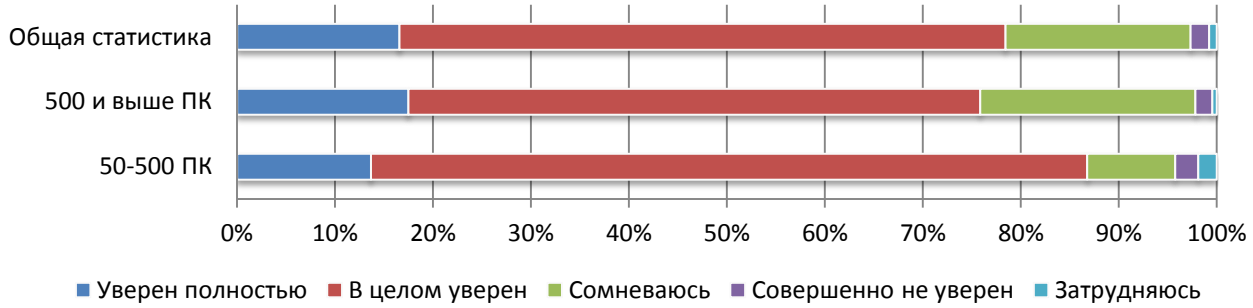


Рисунок 14. Произошедший или предотвращенный инцидент способствует увеличению инвестиций в корпоративную СОИБ.

В том, что наглядная демонстрация произошедшего или предотвращенного инцидента способствует развитию корпоративной СОИБ, уверены 86,7% опрошенных представителей, работающих в средних, и 75,8% респондентов, работающих в крупных компаниях.

> *Это означает, что не требования законодательства или регуляторов, а инцидент остается главным драйвером развития корпоративных систем информационной безопасности.*

Заключение

Системы обеспечения информационной безопасности российских компаний нельзя назвать надежными, если речь заходит о защите от внутренних угроз - уверены участники нашего исследования. При этом люди, ответственные за их надежность, понимают, чем обернется для их работодателей реализация той или иной угрозы. Сотрудники и руководители ИТ- и ИБ-служб точно знают или имеют представление о том, каким образом можно повысить уровень защиты информации, улучшить системы обеспечения информационной безопасности.

Проблема в том, что при оценке масштабов опасности ИТ- и ИБ-службы исходят, в основном, из ценности отдельных типов корпоративной информации, что сказывается на принципиальной разнице карт угроз в различных отраслях. Оценки уровня опасности типов угроз сильно разнятся по выборке в целом (в пределах 4 баллов), но мало отличаются в пределах отрасли.

При этом источник угрозы – **нарушитель – как бы выпадает из поля зрения ИТ- и ИБ-служб**. Уровень опасности различных типов нарушителей, по мнению участников исследования, практически одинаков. Оценки различных типов нарушителей по всей выборке колеблются в пределах полутора баллов.

Складывается ощущение, что ИТ- и ИБ-службы стремятся контролировать действия всех потенциальных нарушителей, которые имеют возможность причинить вред компании. Хотя **более прагматичным представляется подход, когда большее внимание уделяется статистически или субъективно более опасным для бизнеса типам нарушителей** – нелояльным сотрудникам, топ-менеджерам, администраторам, сотрудникам подрядчиков.

> *Для более эффективной защиты информации ИТ- и ИБ-службам необходимо сосредоточить усилия на наиболее «опасных» направлениях, не распылять силы по всему фронту борьбы с нарушителями. Представляется целесообразным выработать комплексный подход, совместив оценку угроз (исходя из ценности информационных активов) и оценку нарушителей (на основе количественной статистики инцидентов).*

Исследование показывает, что реальная картина инцидентов в компаниях мало зависит от размеров организаций, но кардинально отличается от отрасли к отрасли. Иначе говоря, **ИБ-специалист в средней компании обязан уделять проблеме защиты от внутренних угроз не меньше внимания, чем специалист в крупной компании**. Ущерб от реализации того или иного типа внутренней угрозы – от превращения угрозы в реальный инцидент - в средней и крупной компании сопоставим.

Драйвером для развития СОИБ в компаниях по-прежнему остается инцидент. Причем в средних компаниях это проявляется ярче, чем в крупных**. Средний бизнес вообще довольно быстро «набирает зрелость» и способен в ближайшее время стать точкой роста для всего ИБ-рынка**.

С учетом идентичности картины угроз в крупных и средних компаниях в рамках одной вертикали, можно прогнозировать появление большого количества тиражных средств защиты для среднего бизнеса, прошедших «школу» верхнего сегмента – успешно опробованных в крупных организациях. Также очевидно, что повышение уровня безопасности корпоративной информации в российских компаниях возможно за счет фокусирования сил и средств ИТ- и ИБ-служб на защите более ценной информации в сочетании с повышенным вниманием к определенному, потенциально более опасному типу нарушителей.

Глоссарий

Внутренняя угроза ИБ - *к внутренним угрозам относятся любые потенциально возможные действия с информацией, которые (действия) исходят изнутри информационной системы компании (в отличие от внешних, инициированных извне), способны негативно повлиять на целостность, доступность и/или конфиденциальность информации и, как следствие, причинить компании ущерб.*

Инцидент информационной безопасности (ИБ-инцидент) - *событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ. Реализация угрозы ИБ—нарушение свойств ИБ информационных активов (информации) – доступности, целостности, конфиденциальности. ГОСТ Р ИСО/МЭК 27001–2006 Информационная*

технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. /Стандарт ЦБ РФ СТО БР ИББС-1.0-2010.

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 государственной, коммерческой, иных видов тайн.*

Тип нарушителя *– в данном исследовании мы классифицировали субъект инцидента или угрозы – нарушителя – по признаку уровня доступа к информации. Аналитический Центр InfoWatch выделяет пять типов нарушителей – Сотрудник компании, Администратор, Топ-менеджер, Подрядчик. В классификацию добавлен внешний нарушитель. На основе данной классификации формируется карта нарушителя (общая, отраслевая) – диаграмма, отражающая представление ИТ- и ИБ-специалистов об уровне опасности того или иного типа нарушителей.*

- ✓ *Сотрудник компании, имеющий легитимный доступ к охраняемой информации*
- ✓ *Администратор – сотрудник с расширенными правами доступа*
- ✓ *Топ-менеджер – сотрудник, к которому, как правило, применяются более мягкие политики безопасности, чем к рядовому персоналу*
- ✓ *Подрядчик (сотрудник подрядчика) – внешние консультанты, ИТ-персонал на аутсорсинге и пр. – сотрудники, имеющие легитимный доступ к информации и инфраструктуре, но не связанные общекорпоративными правилами информационной безопасности*
- ✓ *Внешний нарушитель – в самом общем смысле источник внешних угроз – вирусных, DDoS атак и пр.*

Тип угроз *– мы классифицировали угрозы по признаку объекта защиты (какая информация может быть скомпрометирована в результате реализации угрозы) и по признаку особенностей действий субъекта (нарушителя). Аналитический Центр InfoWatch выделяет шесть типов инцидентов – Утечка персональных данных, Утечка платежных данных, Утечка ноу-хау, Утечка информации, составляющей коммерческую тайну, Нелояльное поведение сотрудников, Злоупотребление доступом. На основе данной классификации формируется карта угроз (общая и отраслевая) – диаграмма, отражающая представление ИТ- и ИБ-специалистов об уровне опасности той или иной угрозы для бизнеса в случае реализации угрозы (наступления инцидента).*

- ✓ *Утечка персональных данных, Утечка платежных данных, Утечка ноу-хау, Утечка информации, составляющей коммерческую тайну, - в общем случае – утечка информации. Под утечкой мы понимаем действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, повлекшее потерю контроля над информацией или нарушение конфиденциальности этой информации.*
- ✓ *Нелояльное поведение сотрудников – мошенничество, криминальные действия с использованием инфраструктуры работодателя, распространение нежелательной информации, несанкционированное общение с прессой и конкурентами, саботаж, сговоры с целью хищения информационных или материальных активов, получения откатов*

- ✓ *Злоупотребление доступом – нелегитимное хранение информации ограниченного доступа, получение доступа к закрытым для сотрудника информационным ресурсам.*

Карта инцидентов *– диаграмма, составленная на основе данных программных продуктов InfoWatch или данных базы инцидентов Аналитический Центр InfoWatch. Карта инцидентов на основе данных программных продуктов отражает распределение (по количеству) инцидентов шести типов (типы инцидентов совпадают с типами угроз), произошедших за определенный период времени в компании-клиенте InfoWatch и зафиксированных программными продуктами InfoWatch в ходе «пилотной» или промышленной эксплуатации продуктов InfoWatch. Данные предоставлены на условиях анонимности и могут использоваться исключительно для формирования карты инцидента на уровне отрасли. Показывает, какие инциденты ИБ* ***в реальности*** *чаще всего случаются в компании, отрасли, стране. Поскольку инцидент ИБ является реализацией угрозы, в данном исследовании классификация угроз и инцидентов совпадают.*

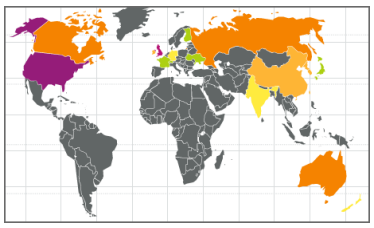
Карта угроз *– по аналогии с картой инцидентов - диаграмма, сформированная по итогам опроса участников исследования. Отражает* ***представления*** *участников опроса о том, что угрожает их компаниям. Классификация угроз совпадает с классификацией ИБ-инцидентов.*

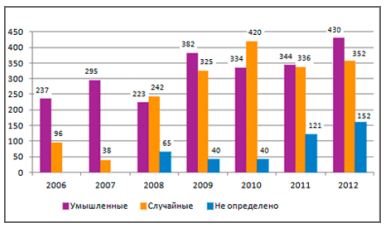
Карта нарушителя *– диаграмма, сформированная на основе результатов опроса участников исследования, где каждому (из пяти) типов нарушителей (см. типы нарушителя) присвоен определенный балл – субъективная оценка опасности для бизнеса этого типа нарушителя, данная участниками исследования. Отражает* ***представления*** *участников опроса об источниках опасности для их компаний.*

Мониторинг утечек на сайте InfoWatch

На сайте аналитического агентства InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты утечек с комментариями экспертов InfoWatch.

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.





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

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитическое агентство InfoWatch

www.infowatch.ru/analytics

Приложение. Таблицы

Таблица 1. Отраслевая карта нарушителей. Оценка участников исследования.

Аналитический Центр InfoWatch опрошено 918 представителей коммерческих компаний и государственных органов (сотрудники и руководители ИТ и ИБ-служб). Респондентам предложено проранжировать типы нарушителей список из 5 типов нарушителей ИБ по степени возможного ущерба для бизнеса. Итоговый балл для отрасли вычислялся методом среднего арифметического.

6 – максимально возможный ущерб. 1 – минимальный ущерб.

	Сотрудник компании	Администратор	Топ-менеджер	Подрядчик	Внешний злоумышленник
Банки и финансы	3,5	4,8	4,1	3,6	3,1
Медицина	2,9	4,6	3,2	1,1	2,4
Торговля, HoReCa	2,7	5,1	4,2	2,5	3,7
ИТ и телеком	3,9	4,8	5,6	4,7	3,8
Промышленность и транспорт	2,9	5,5	4,3	3,8	2,5
Госорганы и силовые структуры	5,9	5,3	1,5	2,1	2,2
Образование	3,2	2,4	2,1	1,3	1,8

Таблица 1. Отраслевая карта нарушителей.

Таблица 2. Отраслевая карта угроз. Оценка участников исследования.

Аналитический Центр InfoWatch опрошено 918 представителей коммерческих компаний и государственных органов. Респондентам предложено проранжировать список из 6 угроз в сфере ИБ по степени возможного ущерба для бизнеса. Итоговый балл для отрасли вычислялся методом среднего арифметического.

6 – максимально возможный ущерб. 1 – минимальный ущерб.

	Утечка персональных данных клиентов/ сотрудников	Утечка платежной информации (пластиковые карты, номера и суммы на счетах)	Утечка промышленных секретов, ноу-хау	Утечка коммерческой информации (коммерческая тайна - договоры, маркетинговые стратегии)	Факты мошенничества, сговора, нелояльного поведения сотрудников (в т. ч. в социальных сетях)	Несанкционированный доступ к информации, нелегитимное использование/ хранение
Банки и финансы	4,2	5,7	1,2	4,9	2,1	5,1
Медицина	5,3	1,6	2,1	3,1	2,3	4,2
Торговля, HoReCa	5,7	5,9	1,2	2,5	3,7	1,1
ИТ и телеком	3,9	4,8	5,6	4,7	3,8	2,9
Промышленность и транспорт	1,9	1,5	5,7	3,2	3,4	1,9
Госорганы и силовые структуры	5,9	1,3	1,4	1,1	2,2	3,3
Образование	3,1	1,9	1,1	1,3	1,8	1,1

Таблица 2. Отраслевая карта угроз.