ИССЛЕДОВАНИЕ

ОСОБЕННОСТИ ОРГАНИЗАЦИИ СЛУЖБЫ ИБ В РАЗНЫХ СФЕРАХ БИЗНЕСА

ОБ ИССЛЕДОВАНИИ

Исследование, проведенное компанией «Инфосистемы Джет», основывается на данных, полученных в ходе реализации проектов по аудиту информационной безопасности в 2019–2021 годах, а также на данных опроса ключевых заказчиков компании.

В рамках подготовки материала мы поставили себе задачу ответить на следующие вопросы:

- Какова численность штата специалистов службы ИБ и в каких компаниях таких специалистов больше всего: в финансовом секторе, промышленности, государственных учреждениях или других сферах?
- Кому чаще всего подчиняется служба ИБ и как это подчинение меняется в зависимости от сферы бизнеса?
- В каких компаниях процессы информационной безопасности наиболее зрелые?

Цель данного исследования — дать возможность компаниям в отсутствие отраслевого бенчмарка по численности службы ИБ сравнить себя с другими игроками рынка, а также получить представление о том, как развита ИБ в той или иной сфере бизнеса.

100 компаний

Для анализа было выбрано 100 компаний среднего и крупного бизнеса, география деятельности которых включает Российскую Федерацию, Азербайджан и Узбекистан. Среди проанализированных компаний — организации финансового сектора (25%), промышленности (18%), топливно-энергетического комплекса (15%), государственные учреждения (8%), сферы страхования (5%), ритейла (7%), телекома (4%), а также иные коммерческие компании (сфера услуг, ИТ-компании, девелопмент, медицина и др) (18%)

Стоит отметить, что так как в выборку попали организации, являющиеся заказчиками «Инфосистемы Джет» по проектам в области ИБ, их зрелость заведомо должна быть несколько выше средней по индустрии, так как они уделяют внимание вопросам ИБ настолько, что хотя бы единожды привлекли внешних консультантов в этой области.

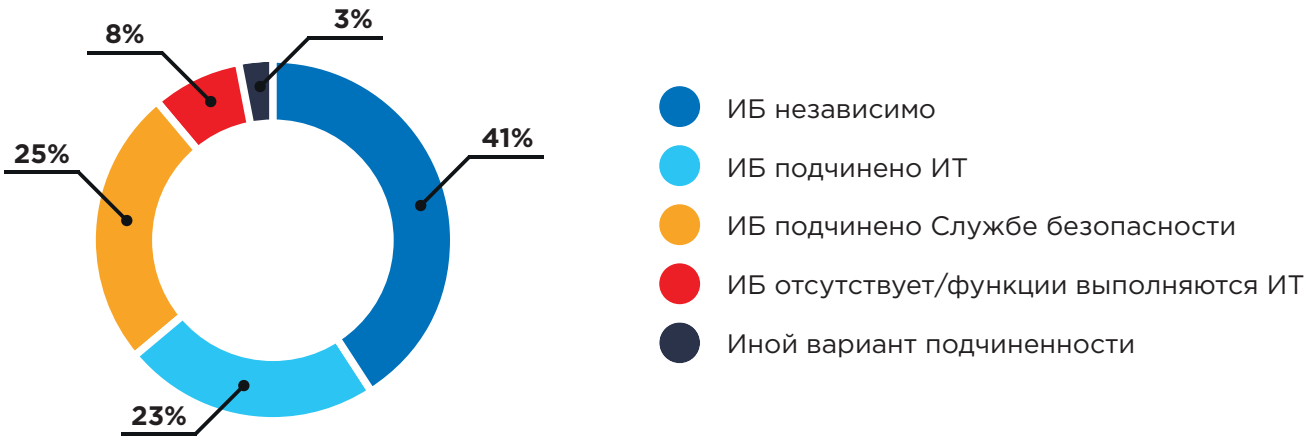
СТРУКТУРА ПОДЧИНЕНИЯ СЛУЖБЫ ИБ

Почти **половина** проанализированных компаний (41%) имеют собственную службу информационной безопасности, подчиненную исполнительному органу. В 23% случаев служба ИБ подчиняется блоку ИТ, в 25% — службе безопасности, 3% имеют иную структуру подчиненности.

Полученные данные значительно отличаются от картины, которую мы наблюдали 5-7 лет назад в российских компаниях. Растет понимание необходимости выведения подразделения ИБ из подчинения службы ИТ или СБ, что подтверждает довольно высокая цифра в 41%.

При этом **только 8%** компаний до сих пор не имеют отдельно выделенного подразделения ИБ. Поддержанием процессов ИБ в таких компаниях, как правило, неформально занимаются работники ИТ, которые рассматривают такие обязанности как дополнительную нагрузку, вследствие чего они выполняются «по остаточному принципу». Такими компаниями обычно являются небольшие организации коммерческого сектора.

Структура подчинения



Практика выделения ИБ-службы в самостоятельное независимо подчиненное структурное подразделение наиболее характерна для предприятий финансового, государственного сектора,сферы страхования и иных коммерческих компаний (сфера услуг, ИТ-услуги, девелопмент, медицина и др).

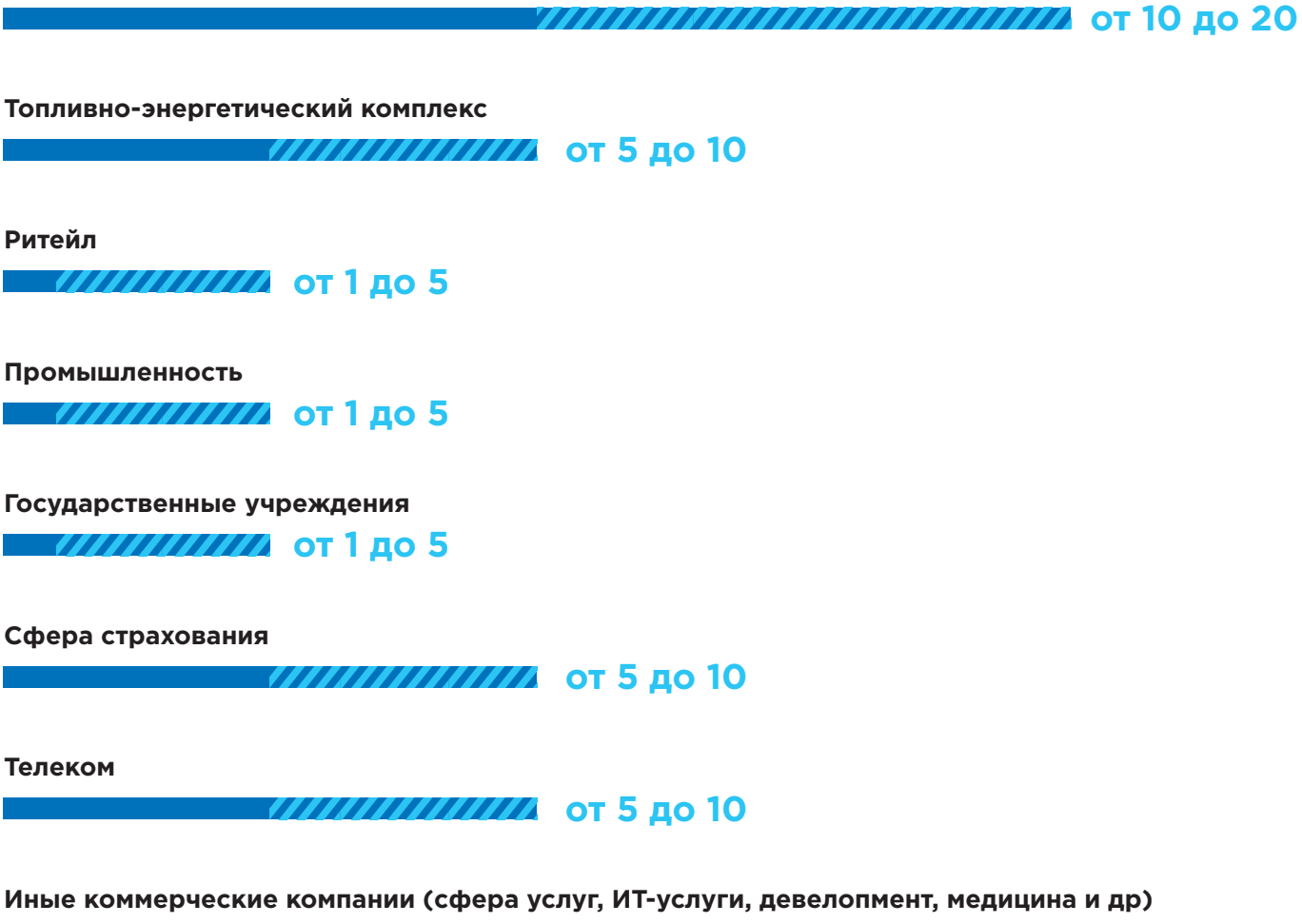
Подчинение департаменту ИТ чаще всего встречается в телекоме и промышленности.

Ситуация, когда ИБ относится к службе безопасности, характерна для топливно- энергетического комплекса и ритейла.

ШТАТНАЯ ЧИСЛЕННОСТЬ РАБОТНИКОВ ИБ

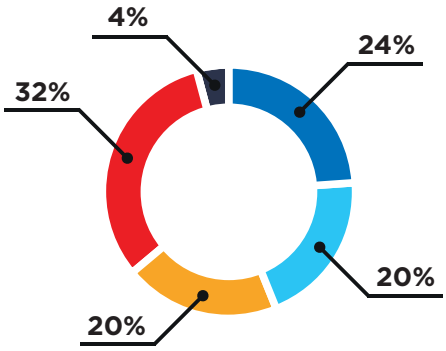
Самая большая численность работников ИБ, как и следовало ожидать, характерна для предприятий финансового сектора. Штат специалистов здесь в среднем находится в диапазоне от 10 до 20 человек, при этом 32% выборки имеет штат более 20 человек. Бизнес таких компаний особенно привлекателен для киберзлоумышленников, а также находится в постоянном фокусе регуляторов, что требует большого числа специалистов для выполнения обязательных требований. Меньше всего штат — в государственных компаниях и компаниях с госучастием: за информационную безопасность в них отвечают зачастую два специалиста, численность штата находится в диапазоне от 1 до 5 человек. Такая ситуация связана в большей степени со сложностью обоснования в данной отрасли необходимости расширения штатного расписания. Медианное значение штата выделенных специалистов ИБ среди всех проанализированных компаний составляет три человека, среднее значение — 6 человек.

Распределение числа специалистов по отраслям

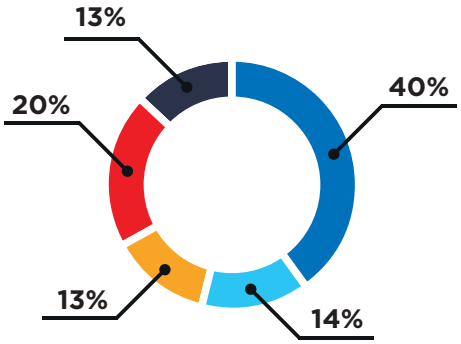


Распределение штата для каждой отрасли

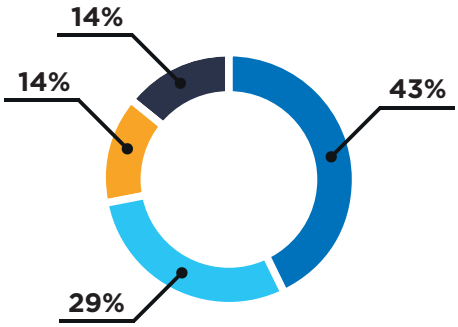
От 1 до 5 | от 5 до 10 | от 10 до 20 | Более 20 | Отсутствует



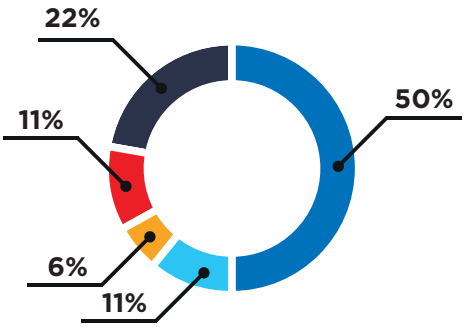
Финансовый сектор



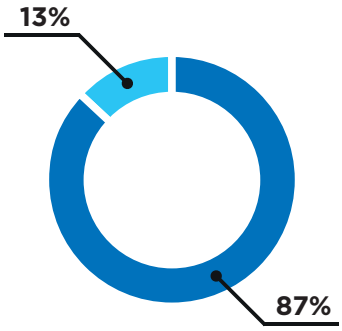
Топливно-энергетический комплекс



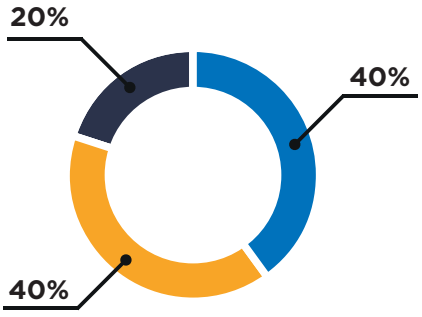
Ритейл



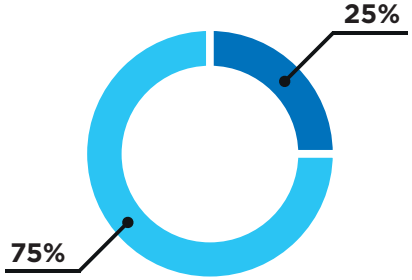
Промышленность



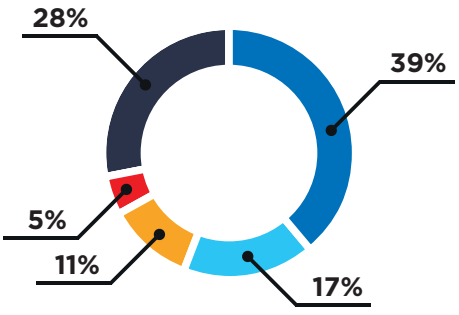
Государственные учреждения



Сфера страхования



Телеком



Коммерческие компании

УРОВЕНЬ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках проведенного исследования также была собрана информация об интегральном уровне зрелости процессов информационной безопасности в различных сферах бизнеса. В качестве инструмента измерения была использована модель Capability Maturity Model Integration (CMMI) — модель совершенствования процессов, характеризующаяся следующими уровнями:

- **0** Отсутствует
- **1** Начальный
- **2** Повторяемый
- **3** Определенный
- **4** Управляемый
- **5** Оптимизируемый

Оценка зрелости по CMMI позволяет приближенно получить предоставление о прогрессе внедрения процессов и технологий ИБ в компании.

Нулевой уровень шкалы (0) означает, что вопросами обеспечения ИБ компания не озадачивалась, финансирование отсутствует, защита обеспечивается встроенными механизмами ИТ-систем.

В рамках начального уровня (1) выполняются единичные процессы, все держится на инициативе отдельных сотрудников, ИБ рассматривается зачастую как чисто техническая задача, специализированные средства защиты информации отсутствуют или представлены в минимальном количестве.

В рамках повторяемого уровня (2) в компании присутствуют минимально необходимые средства защиты, процессы ИБ повторяемы и планируются, однако они не соответствуют общепринятым практикам и плохо управляемы, в том числе из-за недостатка ресурсов.

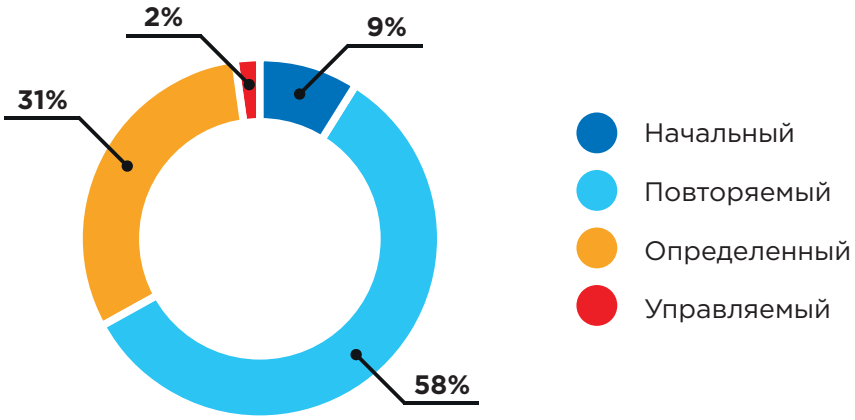
На определенном уровне (3) имеется достаточный объем ресурсов для поддержки и управления процессами ИБ на оперативной основе, разработана программа развития ИБ в перспективе нескольких лет. Процессы стандартизированы и доказали свою надежность, документация разработана и поддерживается в актуальном состоянии.

Управляемый уровень (4) характеризуется наличием инструмента измерения, эффективность процессов измеряется на постоянной основе с помощью набора метрик. Процессы являются измеримыми и контролируемыми. Применяются автоматизированные инструменты, налажена четкая связь с бизнесом.

На последнем, оптимизируемом уровне (5) процессы постоянно улучшаются, измеряются, большая часть задач автоматизирована и соответствует лучшим практикам. ИБ является частью корпоративной культуры.

Большая часть (58%) проанализированных компаний имеет интегральный второй (повторяемый) уровень зрелости.

Уровень зрелости процессов ИБ



Из проанализированных сфер бизнеса наиболее зрелые процессы информационной безопасности имеют компании финансового сектора и крупные ИТ-компании: третий (определенный уровень) имеют порядка 30% таких компаний.

Наименее зрелые процессы отмечены в государственном секторе.

В рамках исследования была также выявлена следующая зависимость уровня зрелости процессов от штатной численности работников ИБ:

1. **Начальный**
   Нет работников
   или **один** специалист
2. **Повторяемый**
   От 1 до 5 специалистов
3. **Определенный**
   5 и более специалистов
4. **Управляемый**
   10 и более специалистов

Оптимизируемый (максимальный, пятый) уровень не был отмечен ни в одной организации.

КРАТКИЕ ВЫВОДЫ

Несмотря на то, что порядка **92%** компаний уже имеют штат собственных специалистов ИБ, общий уровень зрелости по-прежнему остается достаточно низким. Такая ситуация обусловлена как недостатком кадровых ресурсов (медианное значение штата ИБ составляет три человека), так и недостаточным финансированием со стороны бизнеса.

Наиболее зрелыми отраслями традиционно остаются финансовый сектор и крупные ИТ-компании.

Для получения дополнительной информации вы можете
обращаться к **Александру Морковчину**,
руководителю группы департамента консалтинга
центра информационной безопасности компании «Инфосистемы Джет»

security@jet.su

Инфосистемы Джет