Аналитический отчёт

«О вовлечённости первых лиц предприятий в управление информационной безопасностью»

подготовлен экспертной подгруппой
по кибербезопасности НТИ «Энерджинет»

2023 г.

Аннотация

Настоящий отчет подготовлен экспертами подгруппы по кибербезопасности Национальной технологической инициативы «Энерджинет» с целью выявления наиболее острых проблем в области осведомленности и вовлеченности работников и руководства организаций в проблематику обеспечения информационной безопасности (далее ИБ).

В отчёте приведены результаты анализа двух анонимных опросов среди участников сообществ специалистов по информационной безопасности промышленных предприятий в Telegram.

Первый опрос проведён в апреле 2022 года до опубликования Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», которым предписано введение должности заместителя руководителя организации по информационной безопасности и возложение на руководителей персональной ответственности за состояние ИБ в организациях (26 вопросов).

Второй опрос с аналогичными вопросами был проведён в сентябре 2022 года (14 вопросов).

Авторы исследования полагают, что анонимность опроса обеспечила объективность его результатов независимого от конъюнктуры среды или работы в конкретной организации.

Основные направления исследования:

1) Выявить отношение к задачам и требованиям ИБ следующих категорий сотрудников:
   - владельцы бизнеса или их представители в совете директоров;
   - первые лица организации (генеральный директор и C-Level);
2) Собрать мнения в какой степени собственники и руководители участвуют в обеспечении ИБ компании;
3) Выявить и сформулировать существующие проблемы тренды в сфере ИБ;
4) Проанализировать зависимость эффективности подразделения ИБ от подчиненности

Отчёт предназначен для руководителей и специалистов, работающих в сфере информационной безопасности, а также для руководителей организаций, независимо от форм собственности и сферы деятельности.

Результаты исследования

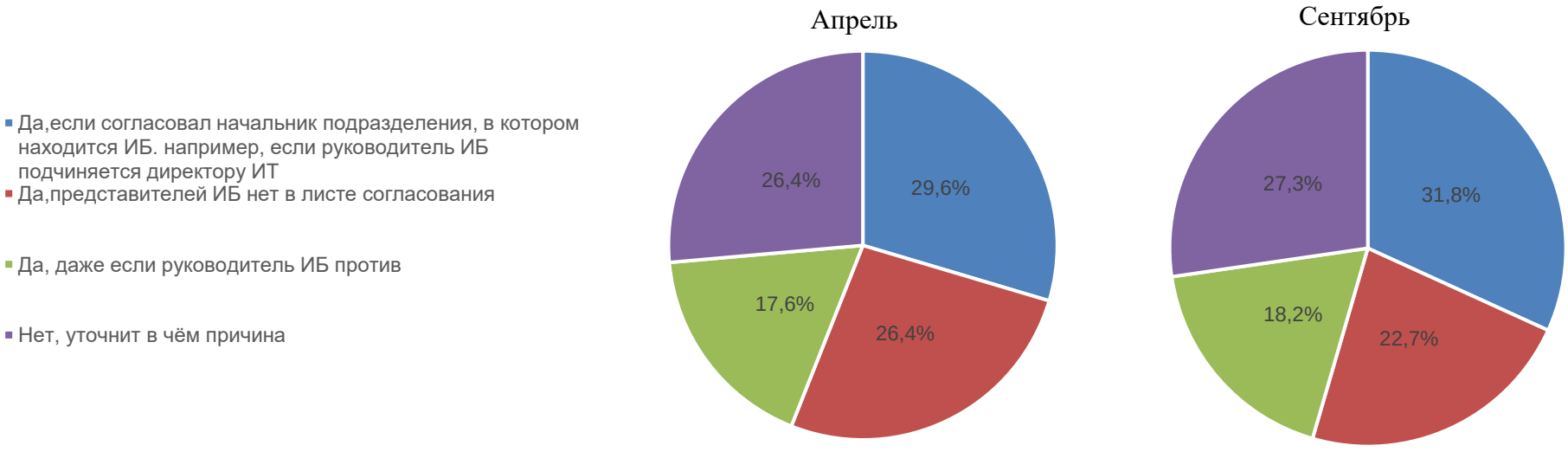
Организационные вопросы

Вовлечённость руководства предприятия в вопросы ИБ во многом связана с доступностью первого лица для руководителя ИБ (с возможностью напрямую докладывать о проблемах, путях их решений, согласовывать планы и бюджеты).

Согласно данным, полученных в ходе подготовки отчёта, лишь треть (34%) генеральных директоров готовы уделять личное внимание данному вопросу.

Принимают участие в работе органов корпоративного управления и участвуют в совещания руководителей организаций 36% руководителей подразделений ИБ.

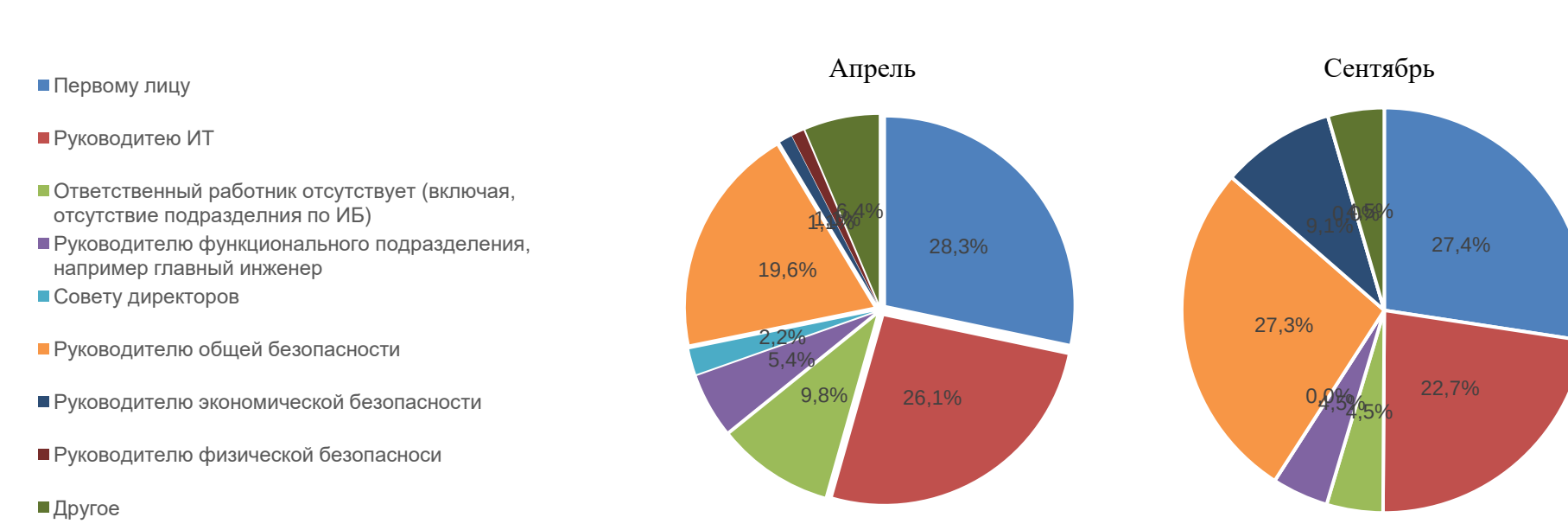
Подписывает ли Первое лицо локальный нормативный акт или договор, если он не согласован ответственным работником/руководителем подразделения по ИБ?



Соответственно, в большей половине организаций (примерно 60%) при подписании договоров и других документов не учитывается мнение руководителей ИБ.

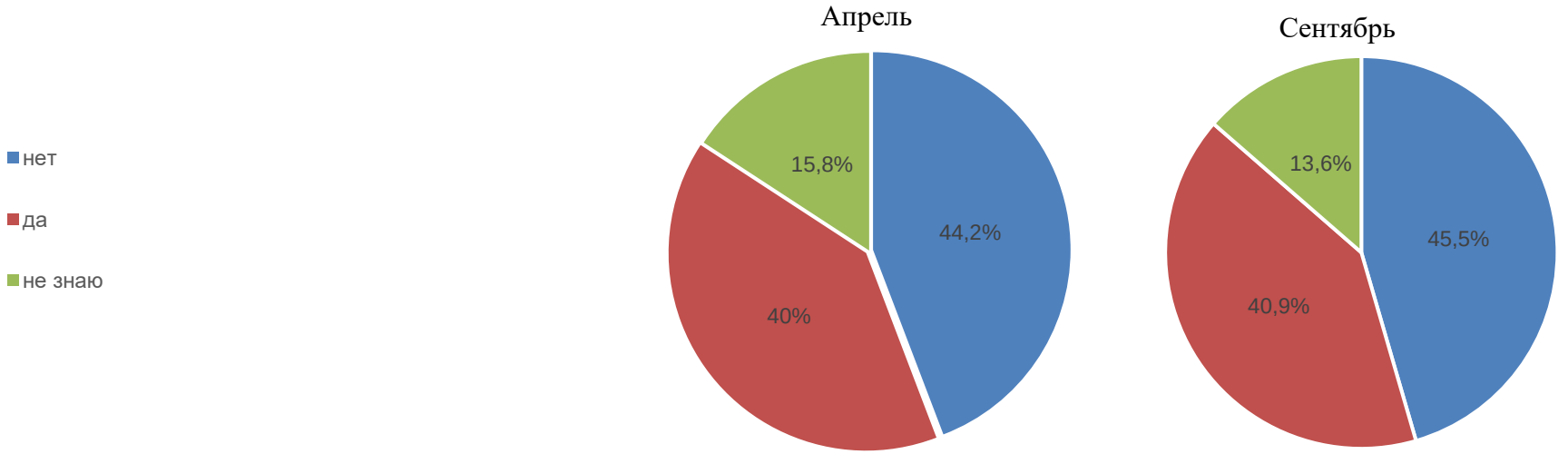
По данным обоих опросов, руководитель ИБ подчиняется первому лицу примерно в 28%, заместителю первого лица по безопасности - 20-27%, практически четверть – 26% подчиняется руководителю ИТ. То есть в последнем случае ИБ сведена до рамок администрирования средств защиты информации, причём это значит, что руководитель ИТ сам определяет политики и требования безопасности к информационным система, сам их выполняет и сам себя проверяет.

Кому в Вашей организации подчиняется ответственный работник/подразделение по ИБ?

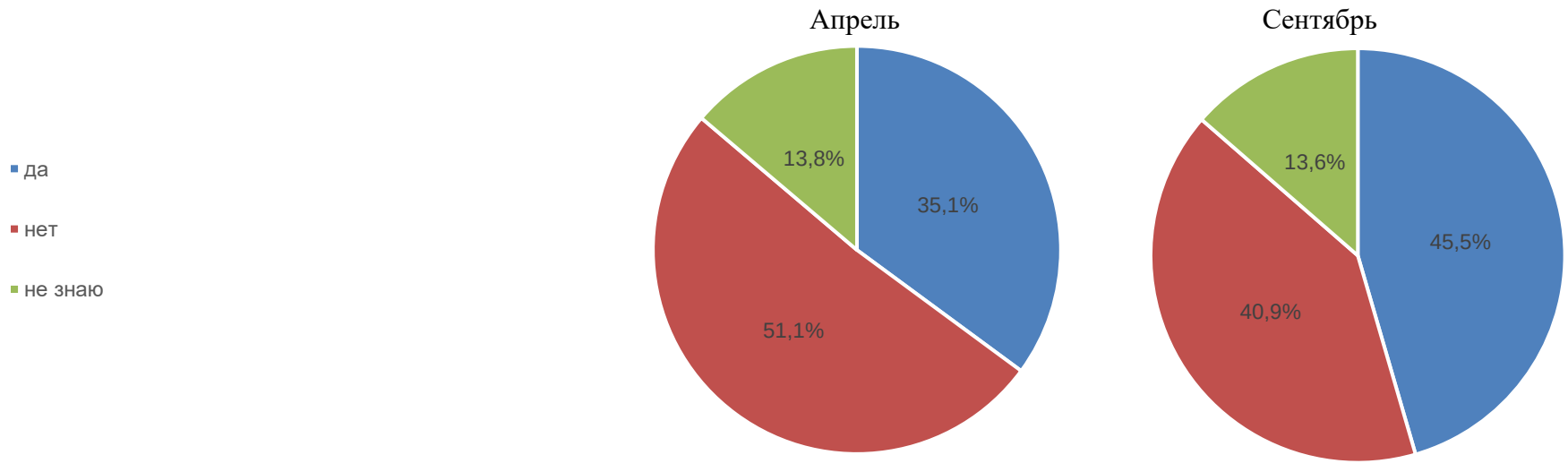


Но на ИБ обращают внимание при принятии решений. Если рассматривать ответы только «да/нет», то половина руководителей организаций и органов корпоративного управления регулярно запрашивают и получают актуальную информацию о состояние ИБ.

Получает/запрашивает ли регулярно первое лицо организации актуальную информацию о состоянии работ по обеспечению ИБ?



Запрашивает ли, анализирует ли ТОП менеджмент информацию о влиянии на состояние ИБ (риски, стоимость обеспечения ИБ, необходимость обеспечения ИБ) при принятии решений о реализации новых инициатив в организации, в т.ч.

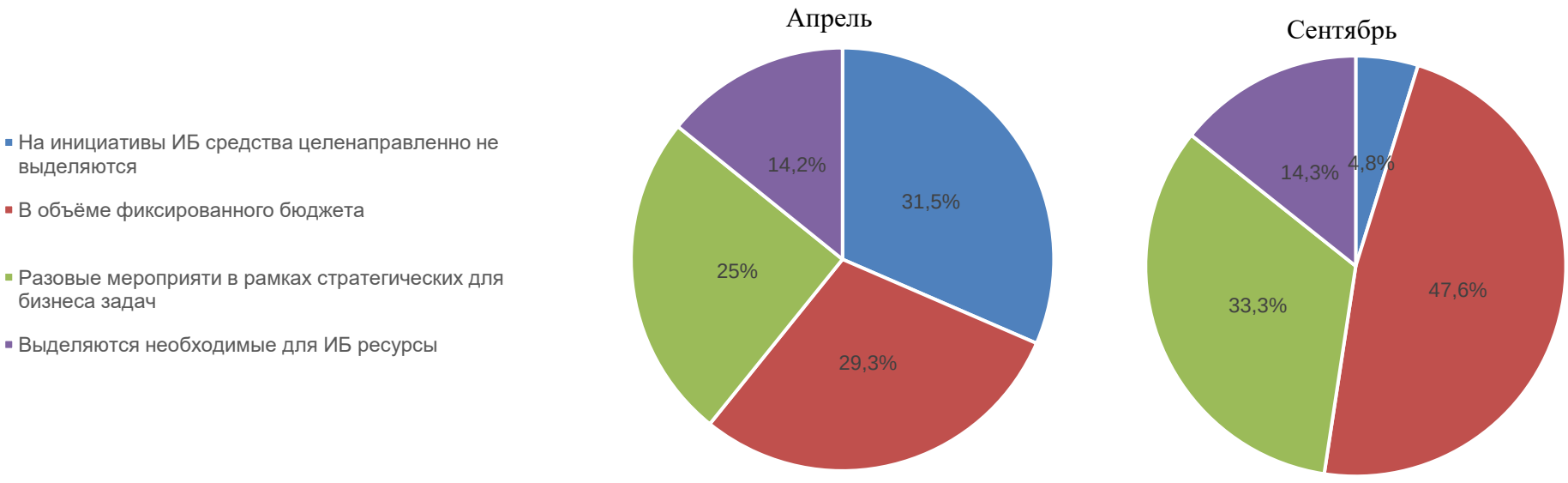


При этом та половина, что запрашивает информацию, использует, анализирует информацию, о состоянии ИБ, о имеющихся рисках при принятии решений о реализации новых инициатив в сфере деятельности организации в целом: изменения процессов, расширения областей деятельности и т.д.

Ключевые точки внимания первых лиц:

Опросы показывают, что ИБ стало лучше финансироваться и в 95% организаций так или иначе средства на повышение защищённости выделяются.

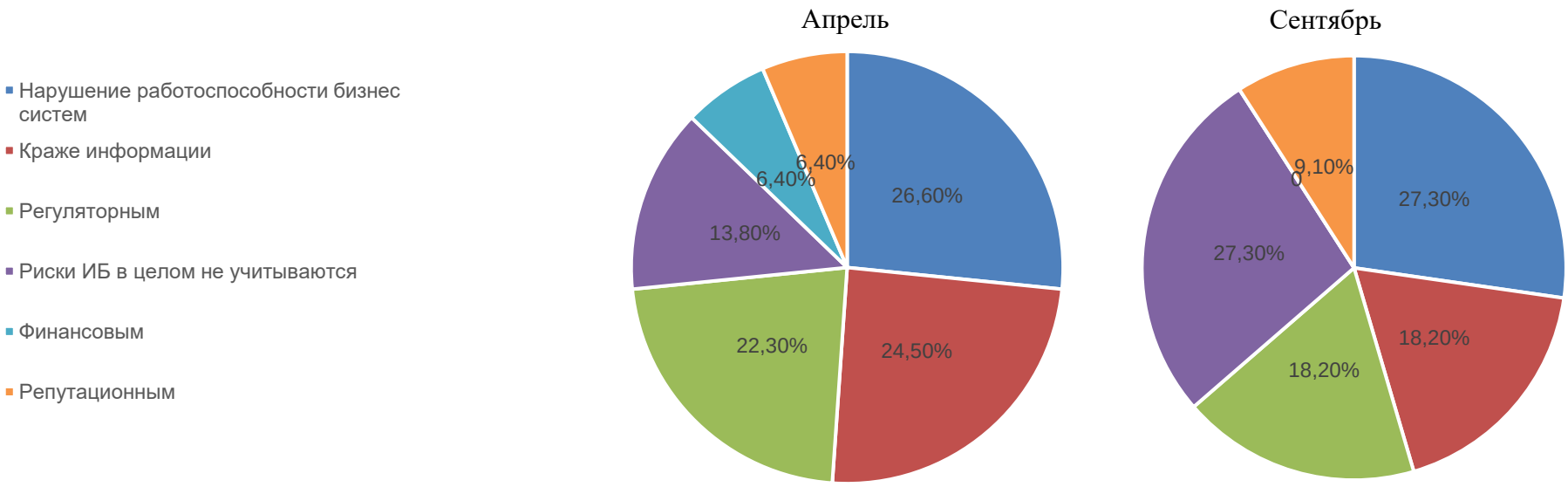
В каком объеме ТОП менеджмент готов выделять ресурсы на решение задач ИБ?



Так как выше уже было выявлено, что не все компании учитывают ИБ при принятии решений, то анализируя ответы о фокусах внимания ТОП-менеджмента и не рассматривая ответ «Риски ИБ не учитываются», можно сделать вывод, что особое внимание уделяется ИБ рискам, связанным с нарушением работоспособности бизнес-систем, и возможной кражей (утечкой) информации, а также вопросам соблюдениям законодательства. Это противоречит распространенному мнению, что ИБ работает только в связи со страхом перед регуляторами.

Риски санкций, а также потенциальные финансовые и репутационные потери интересуют значительно меньше.

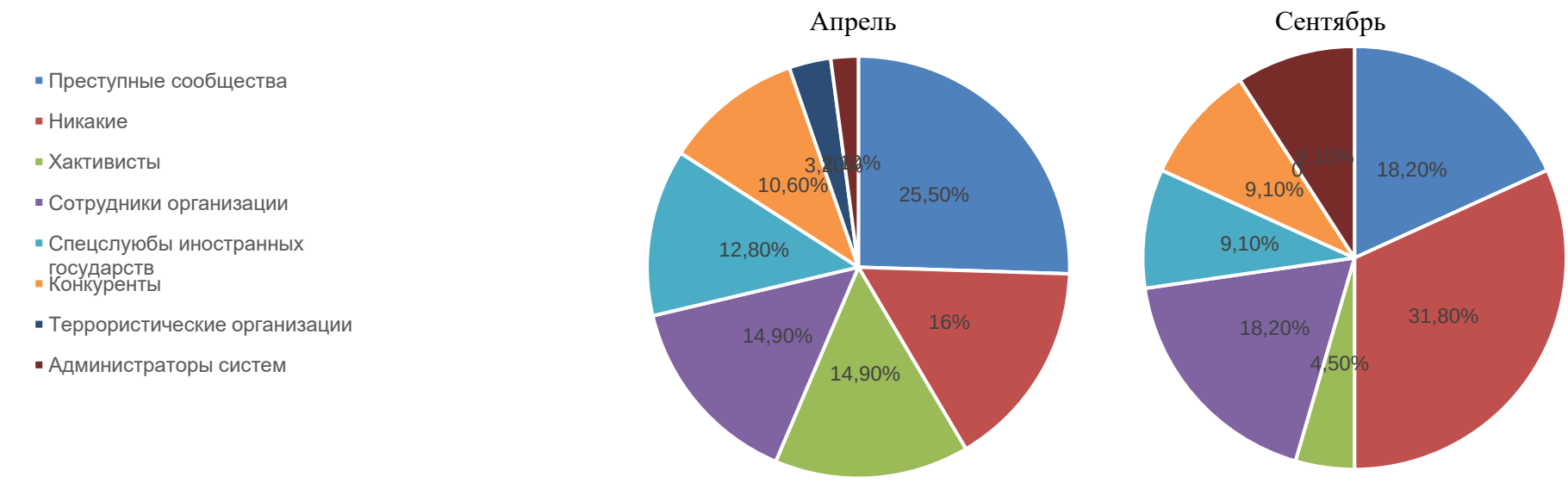
Каким связанным с ИБ рискам отдается приоритет ТОП менеджментом и советом директоров при принятии решении о минимизации рисков?



Интересно, что чаще всего в качестве нарушителя рассматриваются преступные сообщества – их назвали более четверти опрошенных, а конкуренты – в два с половиной раза реже (10,6%), примерно по 15-18% – за рядовыми сотрудниками и хактивистами. Интересно увидеть 9,1-12,8 % голосов в отношении спецслужб, возможно, это предприятия оборонного комплекса.

При повторном опросе на первое место поднялся ответ «никакие», который в расширенном варианте подразумевал, что «есть более простые способы нанести вред организации, нас никто не будет атаковать через ИТ-системы». Это особенно странно на фоне массовых кибератак, обрушившихся на страну после 24.02.2022 г. Но вместе с тем, также сократился процент «хактивистов» и выросла доля «администраторов», можно предположить: занявшись ИБ, значительное внимание стало уделяться внутренним сотрудникам и процессам.

Какой тип злоумышленника рассматривается/признаётся ТОП менеджментом?



Выводы

За исследуемые полгода видно увеличение внимания к ИБ. Вместе с тем, по результатам исследования, необходимо отметить:

1. 28% руководителей ИБ подчиняются первому лицу, заместителю директора по безопасности - 20-27%, практически четверть – 26% – подчиняется руководителю ИТ.
2. 34% генеральных директоров системно уделяют личное внимание задачам ИБ, что говорит об их важности на сегодняшний день.
3. 36% руководителей подразделений ИБ принимают участие в работе органов корпоративного управления и участвуют в совещания руководителей организаций.
4. В четверти организаций при подписании договоров и других документов не учитывается мнение руководителей ИБ, что в целом соответствует доли опрошенных, по мнению которых их компании вообще не уделяют внимание ИБ.
5. Почти во всех организация выделяются средства на ИБ, хотя ранее 30% респондентов фиксировала отсутствие выделения средств.
6. Больше половины руководителей организаций и органов корпоративного управления регулярно запрашивают и получают актуальную информацию о состояние ИБ и вникают в формируемые службой ИБ меры по повышению защищённости предприятия, участвуют в выработке решений в области обеспечения ИБ организации.
7. ТОП-менеджмент уделяет особое внимание рискам, связанным с нарушением работоспособности бизнес-систем, кражей (утечкой) информации и нарушением законодательства.
8. В качестве нарушителя в основном рассматриваются:
   - преступные сообщества – их назвали более четверти опрошенных,
   - рядовые сотрудники,
   - конкуренты и спец. службы иностранных государств.

Для полноты картины стоит учитывать открытые доклады с крупных мероприятий конца 2022 года, таких как SOC форум, а также результаты расширенной встречи экспертной группы по кибербезопасности Ассоциации цифровой энергетики, на которых присутствовали и выступали регуляторы. Общий посыл с мероприятий сводился к тому, что в этом году первые волны атак в целом промышленные компании перенесли нормально, но необходимо усиливать информационную безопасность и готовиться к более серьёзным воздействиям.

Если смотреть изменения за последние 10 лет, то почти половина промышленных предприятий имеет развитую систему информационной безопасности. Причём треть первых лиц включает вопросы управления ИБ в свой фокус внимания.

Вместе с тем, значительных изменений в подходах первых лиц компаний к вопросам информационной безопасности между опросами не выявлено. Скорее всего, те, кто пересмотрели свою политику к ИБ в конце первого квартала, так и работали дальше. Те, кто не прорабатывал вопросы информационной безопасности ранее, до сих пор проводят активный анализ нормативной базы и работают только в юридической плоскости по вопросам ИБ

Отчет подготовлен рабочей группой в составе:
А .А . Боровский, А .В . Петухов, Д .И . Правиков, М .Б . Смирнов,