ИБ по правилам: как российские компании выполняют требования регуляторов к защите информации

kaspersky активируй будущее

Январь, 2025

Описание исследования

Цель исследования

- Выяснить, с какими трудностями сталкиваются компании на российском рынке при выполнении требований законодательства в области информационной безопасности (ИБ).
- Определить наиболее популярные средства защиты информации (СЗИ), используемые при выполнении требований ИБ-законодательства.

Методология

CATI – опрос

Размер выборки

100 компаний

Аудитория

ИТ- и ИБ-специалисты крупных российских компаний и госкорпораций, которые вовлечены в процесс выполнения нормативных требований в области информационной безопасности (ИБ). В исследовании приняли участие представители компаний из разных секторов экономики:

Размер компаний

89%
работают в компаниях с 250+ сотрудников

Отрасль

30%
в компаниях промышленного сектора,

20%
в компаниях государственного сектора,

20%
в компаниях финансового сектора

Следование международным стандартам

40%
в компаниях, которые следуют международным стандартам в области ИБ, например, ISO/IEC 27000

Принадлежность к объектам КИИ

24%
в компаниях, которые относятся к объектам критической информационной инфраструктуры

Основные выводы

Нормы ИБ-законодательства

- Большинство компаний считают существующее регулирование в области ИБ оправданным (81%) и выполнимым (63%).
- При этом более половины специалистов (68%) полагают, что компании в их отрасли соблюдают не все требования ИБ-законодательства. Более «законопослушные» в этом вопросе отрасли – государственная и финансовая.

Трудности при выполнении ИБ-законодательства

Трудности при интерпретации и применении конкретных нормативно-правовых актов связаны с:

- нехваткой квалифицированных кадров — 46%,
- отсутствием понятных инструкций по применению нормативно-правовых актов (НПА) — 44%.

СЗИ для выполнения требований в области ИБ

- Для выполнения требований ИБ-законодательства чаще всего используют средства антивирусной и криптографической защиты (81% и 78% соответственно), защиту почты (70%). Практически половина компаний (49%) использует систему анализа сетевого трафика (Network Traffic Analysis, NTA), 44% респондентов сообщили, что в их организации применяются межсетевые экраны. Наиболее зрелые в плане ИБ компании упоминают такие решения, как система анализа и управления событиями безопасности (Security Information and Event Management, SIEM), используемая в каждой третьей компании, и решения для защиты АСУ ТП, необходимые промышленным предприятиям.
- Среди других мер, проводимых для выполнения требований ИБ, распространены аудиты ИБ (67%) и обучение сотрудников (63%).

Основные выводы

Тенденции по отраслям

Компании финансового сектора более осторожны, видят больше рисков для бизнеса из-за нарушения требований к ИБ, поэтому в индустрии высокий уровень соблюдения норм ИБ. Текущий размер штрафов считают оправданным, при этом полагают, что требования будут ужесточаться, а вместе с этим расти и штрафы. Есть потребность глубоко погрузиться в нормативный вопрос: используют множество источников информации, обращаются за консультациями к внешним экспертам, нуждаются в разнообразных возможностях информирования по требованиям ИБ-законодательства. Сохраняется потребность в разборах отраслевых требований по ИБ: именно недостаточная информированность о правовых нормах ИБ часто является причиной несоблюдения требований. Используют комплексные меры для защиты информации: разнообразные СЗИ и организационные мероприятия.

Представители промышленного сектора чувствуют себя более расслабленно: не ожидают ужесточения требований, видят меньше вероятных негативных последствий за несоблюдение норм ИБ для бизнеса. При этом исполнению норм ИБ в отрасли во многом мешает низкая квалификация специалистов. Среди СЗИ активно используются ТОП-3 популярных инструмента, а в качестве дополнительных мер акцент в отрасли делается на аудиты информационной безопасности.

Представители государственного сектора считают, что в их отрасли компании достаточно строго соблюдают ИБ-законодательство, выполняя все или почти все требования регуляторов. Рисков из-за несоблюдения норм госсектор видит достаточно много. Однако недостаток бюджета часто приводит к нарушению норм ИБ. Вероятно, поэтому и вопрос размера штрафов за нарушения требований ИБ-законодательства для отрасли болезненный: штрафы кажутся оправданными лишь частично или завышенными. Специалисты из госсектора заинтересованы в получении рекомендаций регуляторов по выбору средств защиты информации. При этом они не испытывают сложностей из-за отсутствия инструкций по применению НПА (с чем сталкиваются компании в других индустриях).

Сотрудники госсектора активно используют специализированные источники информации по ИБ, нехарактерные для компаний из других отраслей: различные государственные правовые акты, данные от Роскомнадзора и другие официальные источники. Также при применении конкретных НПА особенно актуальны проблемы с интерпретацией юридических терминов и формулировок в сфере ИБ. Среди СЗИ, наряду с популярными инструментами (средства антивирусной и криптографической защиты информации, защита почты, сканер уязвимостей), около трети компаний используют межсетевые экраны следующего поколения (NGFW), SIEM, в более редких случаях системы противодействия целевым угрозам (Anti-APT), что свидетельствует о достаточно высоком уровне зрелости и экспертизы госкомпаний в ИБ.

1

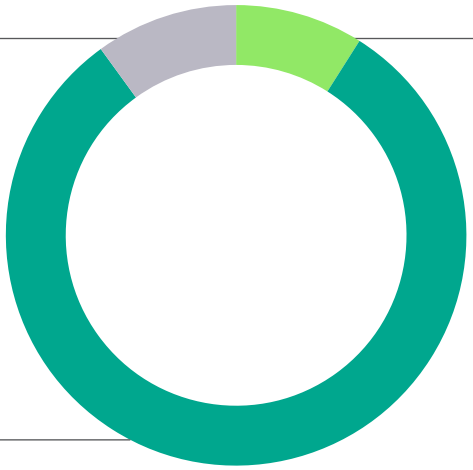
Знакомство с нормативными требованиями

Отношение к нормативно-правовым требованиям в сфере ИБ

Большинство компаний считает существующее регулирование **уместным** в текущих условиях рынка. Лишь небольшая доля компаний сообщает либо о чрезмерности, либо о недорегулированности сферы информационной безопасности.

10%
Требования занижены

9%
Требования завышены

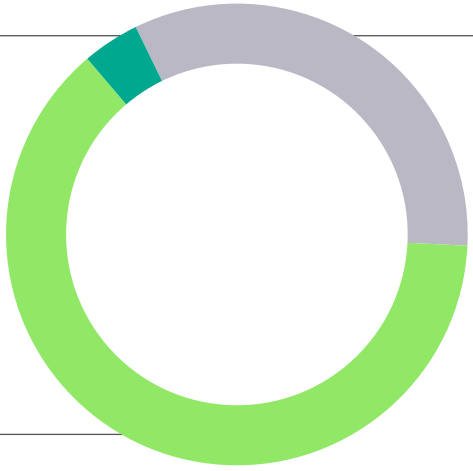


81%
Требования соответствуют рыночным условиям

Более двух третей компаний сообщают о **выполнимости** требуемых норм информационной безопасности. Сложности с исполнением норм испытывает треть компаний.

4%
Легко

33%
Сложно

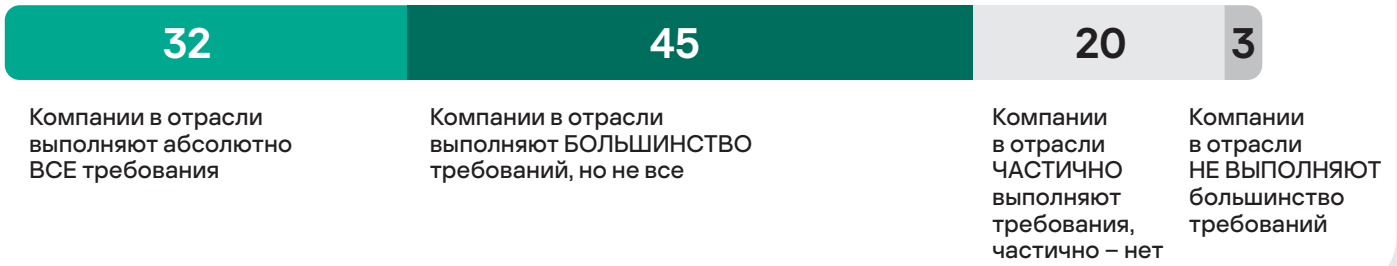


63%
Выполнимо

Субъективная оценка выполнения норм ИБ среди компаний разных секторов

Большинство специалистов считают, что компании в той или иной степени игнорируют нормы ИБ-законодательства, выполняя их не полностью.

Представители **государственного и финансового секторов** считают, что в их сферах компании более строго соблюдают ИБ-законодательство, выполняя все или почти все требования. Представители **промышленного сектора** не настолько уверены в этом: полагают, что многие предприятия соблюдают большинство требований, но есть и те, кто выполняет их частично или только их малую часть.



Компании в отрасли...	Промышленный сектор (N=30)	Государственный сектор (N=20)	Финансовый сектор (N=20)
...выполняют абсолютно ВСЕ требования	5	8	9
...выполняют БОЛЬШИНСТВО требований, но не все	17	9	10
...ЧАСТИЧНО выполняют требования, частично – нет	7	2	1
...НЕ ВЫПОЛНЯЮТ большинство требований	1	0	0
Затруднились ответить	0	1	0

В таблице указано количество людей, выбравших данный вариант ответа

N — общее количество ответивших представителей отрасли

В промышленном секторе менее строго относятся к выполнению ИБ-законодательства, хотя большинство норм скорее исполняется

Госсектор и финсектор более трепетно относятся к исполнению норм ИБ-законодательства, почти половина экспертов считают, что компании выполняют все требования

Основные источники информации о требованиях по кибербезопасности

самые популярные ответы по всем компаниям

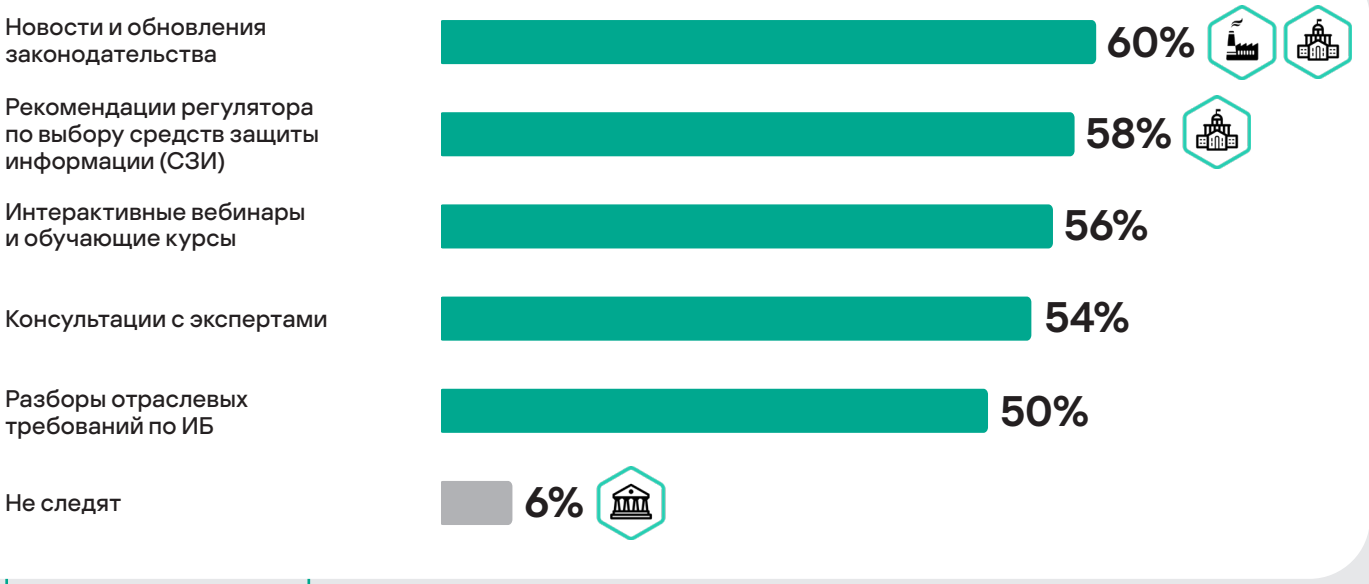
Независимо от отрасли, в которой работает компания, общедоступные информационные ресурсы являются самым популярным источником информации о требованиях по кибербезопасности.

Помимо этого более половины компаний также посещают специализированные мероприятия, используют собственные базы информации и обращаются к внешним экспертам.

Специалисты из **финсектора** используют большее количество источников информации, чем представители других индустрий.

Сотрудники из **госсектора** также упоминали, что обращаются к различным государственным правовым актам, данным от Роскомнадзора и другим официальным источникам.

Дополнительные источники информации о требованиях по кибербезопасности



самые популярные ответы в этом секторе

Большинству специалистов интересны разные источники информирования по требованиями законодательства в ИБ.

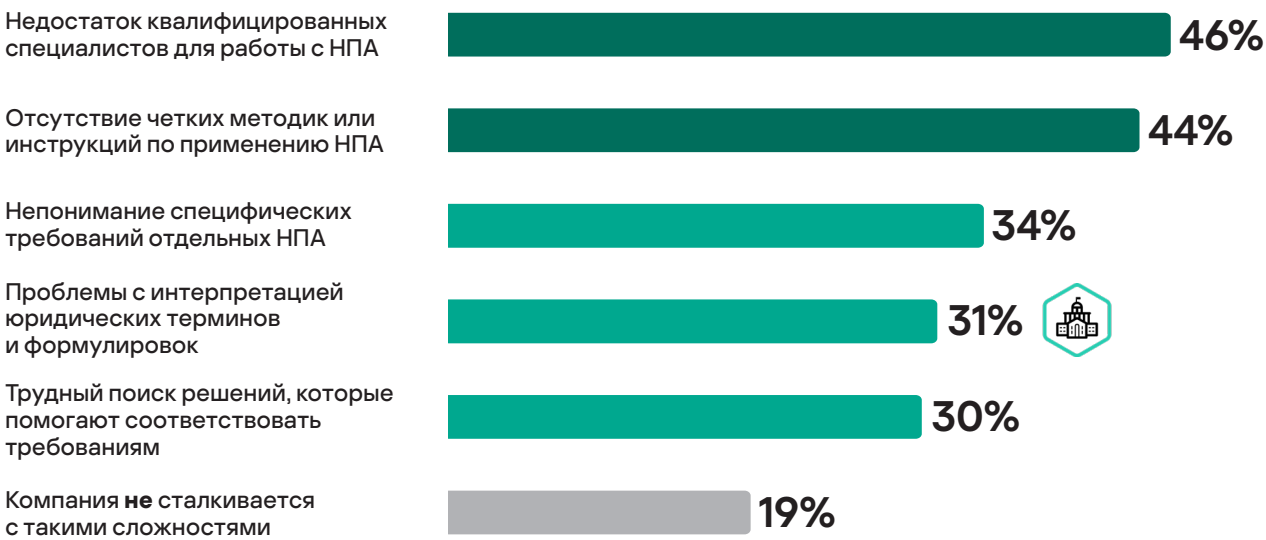
В **государственном** секторе больше, по сравнению с остальными индустриями, обращают внимание на рекомендации по выбору СЗИ, а у **финсектора** есть запрос на разборы отраслевых требований по ИБ. Также представители этого сектора чаще интересуются консультациями с экспертам, чтобы с их помощью разбираться в требованиях ИБ-законодательства.

Можно сказать, что **финсектор** больше, чем другие отрасли, нуждается в разнообразных возможностях информирования по требованиям ИБ-законодательства.

2

Сложности и вызовы

Сложности при интерпретации и применении нормативно-правовых актов в сфере ИБ



самые популярные ответы в этом секторе

самые популярные ответы по всем компаниям

При интерпретации и применении конкретных нормативно-правовых актов (НПА) в сфере ИБ ключевые трудности – это отсутствие специалистов с необходимой квалификацией, а также стандартов применения НПА (хотя для **госсектора** отсутствие инструкций по применению НПА – наименьшая из трудностей).

В единичных случаях специалисты отмечали следующие трудности: нехватка квалифицированных ИТ-специалистов (3 ответа), проблемы с финансированием (2 ответа).

Негативные последствия несоблюдения требований в области ИБ

Финансовый сектор больше остальных встревожен возможными рисками, связанными с требованиями к ИБ. Его представители чаще отмечают различные негативные последствия для бизнеса в случае нарушения норм в области ИБ.

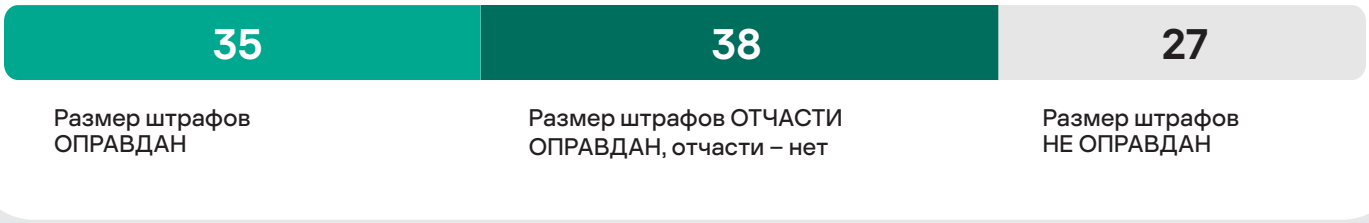
При этом представители **всех индустрий** воспринимают риски ИБ-инцидентов и возможные предупреждения как наиболее вероятные последствия для бизнеса.

Уголовная ответственность – наименее вероятный сценарий с точки зрения опрошенных специалистов, но в меньшей степени о ней беспокоится **промышленный сектор,** который также в целом наиболее оптимистичен в оценке потенциальных рисков.

Потенциальные негативные последствия для бизнеса	Промышленный сектор	Государственный сектор	Финансовый сектор
Штрафы		●	●
Предупреждения	●	●	●
Уголовная ответственность			
Риски ИБ-инцидентов	●	●	●
Нарушения непрерывности бизнес-процессов			●
Другие последствия			

● Более половины представителей сектора оценивают вероятность соответствующего последствия несоблюдения требований как высокую или среднюю

Отношение к штрафам за несоблюдение норм ИБ



Отношение к размерам штрафов за нарушение норм информационной безопасности умеренно разнится между секторами экономики.

Лояльнее всего высказались представители **финансового сектора,** в целом посчитав размер штрафов оправданным, тогда как у специалистов из **госсектора** мнения разделились.

Размер штрафов	Промышленный сектор (N=30)	Государственный сектор (N=20)	Финансовый сектор (N=20)
...оправдан	7	4	9
...отчасти оправдан, отчасти – нет	10	8	7
...не оправдан	6	7	2
Затруднились ответить	7	1	2

В таблице указано количество людей, выбравших данный вариант ответа
N — общее количество ответивших представителей отрасли

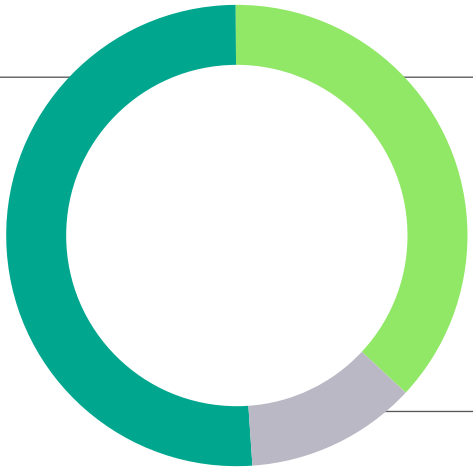
Отношение к нормативно-правовым требованиям в сфере ИБ

Половина специалистов считает, что в течение следующего 2025 года штрафы увеличатся. Около трети полагают, что размер штрафов сохранится на прежнем уровне.

Рост штрафов за несоблюдение норм в сфере ИБ в течение 2025 года...

51%
Ожидают

37%
Не ожидают



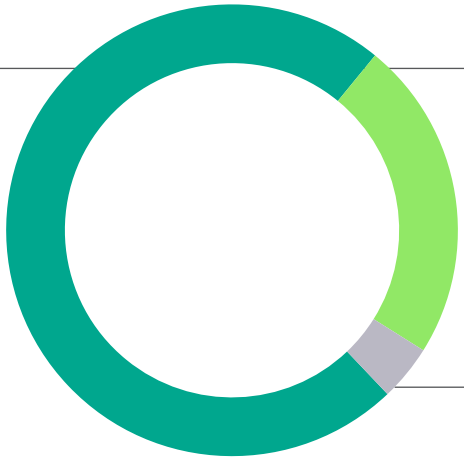
12%
Затрудняются ответить

Большинство специалистов прогнозируют ужесточение правовых норм. В этот сценарий верят больше представители **финсектора,** чем специалисты из **промышленности.**

Ужесточения правовых норм в сфере ИТ в целом, и в сфере ИБ в частности...

73%
Ожидают

23%
Не ожидают



4%
Затрудняются ответить

3

Классы решений СЗИ и мероприятия, способствующие выполнению требований

Рейтинг средств защиты информации для выполнения требований в области ИБ

самые популярные ответы в этом секторе

самые популярные ответы по всем компаниям

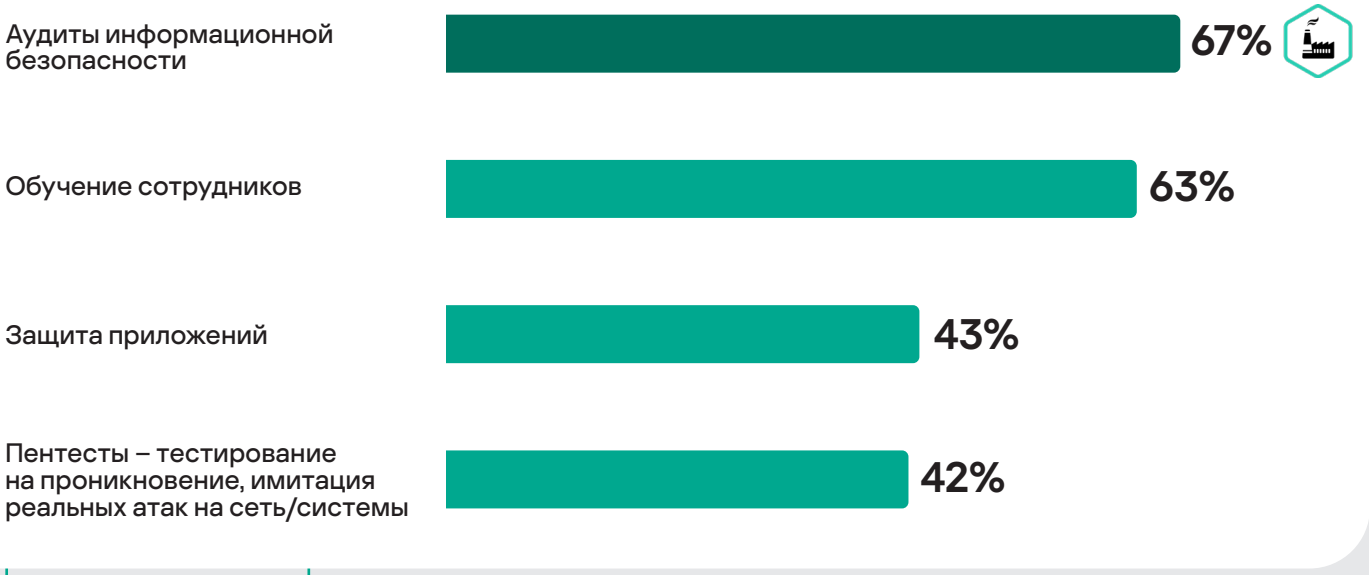
Наиболее популярными средствами защиты информации среди **всех индустрий** являются средства антивирусной и криптографической защиты, усиление защиты корпоративной переписки, а также использование сканера уязвимостей (последний менее важен для **промышленного сектора**).

Финансовый сектор склонен использовать наиболее масштабный комплекс средств по защите, особенно актуальны для этой индустрии SIEM-системы и анализаторы сетевого трафика (NTA).

Также наиболее зрелые в плане ИБ организации упоминают такие решения, как EDR, Anti-APT и специальные решения для защиты АСУ ТП в промышленных компаниях.

Более 40% организаций в России уже используют межсетевые экраны. Кроме того, зрелые в плане ИБ организации упоминают SIEM (каждый третий) и XDR (каждый пятый респондент).

Рейтинг дополнительных организационных мер защиты в области ИБ



самые популярные ответы в этом секторе

самые популярные ответы по всем компаниям

Основные организационные методы, которые наравне с СЗИ используют специалисты ИБ, – это аудиты ИБ и дополнительное обучение сотрудников.

Финансовый сектор в равной степени усиливает информационную безопасность компаний посредством разных методов, используя комплексный подход.

Промышленный и государственный сектора больше уделяют внимания аудитам ИБ и обучению и в меньшей степени – пентестам и дополнительной защите приложений.

Регуляторный хаб знаний в области информационной безопасности

«Лаборатория Касперского» разработала Регуляторный Хаб — незаменимый инструмент, который объединил законы, нормативы и требования по информационной безопасности на одной платформе с удобной системой фильтрации и наглядным отображением взаимосвязей. Он предоставляет бизнесу возможность легко определять основные меры защиты с учетом отраслевой специфики. Ресурс помогает подобрать необходимые для выполнения требований решения «Лаборатории Касперского», что позволяет эффективно противостоять киберугрозам и минимизировать правовые риски.

Регуляторный хаб эффективно используется организациями из различных отраслей. Он упрощает навигацию по законодательству в области ИБ и помогает обеспечивать надежную защиту своих активов в соответствии с требованиями регулирующих органов.

Автоподбор нормативных документов: поможем понять, что необходимо именно вашему бизнесу для соответствия законодательству

Интерактивная база знаний: покажем взаимосвязь между документами, подберем необходимую информацию, чтобы вам не пришлось изучать десятки страниц законов, приказов и т. д.

Практические ИБ-советы: подберем решения для обеспечения информационной безопасности с учетом требований законодательства

Узнайте в несколько кликов все требования регуляторов к вашему бизнесу и получите рекомендации по их выполнению

https://regulhub.kaspersky.ru/