Почему топ-менеджерам нужен специальный тренинг по IT-безопасности

Кибер-безопасность для руководителей

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Security Awareness

Кибербезопасность для руководителей

Успешные кибератаки и утечки данных доставляют немало головной боли IT-отделу и приводят к небольшим перебоям в работе внутренних систем (в лучшем случае). В худшем случае они могут полностью уничтожить вашу компанию. Чтобы оставаться на шаг впереди и не опасаться киберугроз, необходимо активное участие не только руководства по информационной безопасности и IT-отдела, но и руководителей, не занимающихся техническими вопросами.

Высшее руководство является отличной целью для киберпреступников, так как ему доступны максимальные уровни доступа и конфиденциальная информация. Когда речь идет о топ-менеджерах, пробелы в знаниях в области кибербезопасности, нехватка базовых навыков цифровой грамотности и банальные ошибки выливаются в огромные убытки для бизнеса.

Понимают ли друг друга руководители высшего звена и службы IT-безопасности?

Совместная работа этих двух подразделений идет на пользу любой компании, однако лишь 50% IT-директоров считают, что высшее руководство осознает все риски, связанные с киберугрозами. Только 9% руководителей служб безопасности считают, что им удается достичь желаемого результата, сообщая о рисках кибербезопасности совету директоров и другим руководителям высшего звена[1]. А 76% руководителей признаются, что обходили как минимум один из протоколов безопасности своей организации, чтобы сделать что-то быстрее[2].

Из-за такого подхода вопрос финансирования службы ИБ входит в тройку самых сложных тем, с которыми IT-отделы обращаются к руководителям высшего звена. 62% менеджеров признают, что разногласия между службой безопасности и руководством привели как минимум к одному киберинциденту в их компании[3].

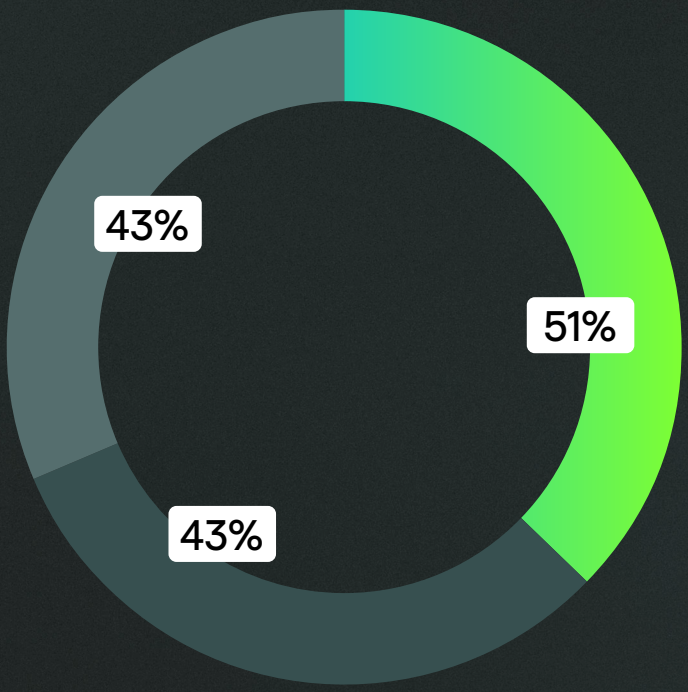
Необходимость знаний

Цифровые технологии все глубже проникают во все сферы нашей жизни. Они открывают новые возможности, помогают сокращать расходы и выходить на новые рынки, а также дают множество других преимуществ. Но, чтобы извлечь максимум пользы из инноваций, необходимы знания и практические навыки в области кибербезопасности.

[1] https://www.ponemon.org/userfiles/filemanager/bkox4uly18udll2ydgyg
[2] Forbes Cybersecurity's Greatest Insider Threat Is In The C-Suite
[3] Исследование Fluent in Infosec. «Лаборатория Касперского», 2023

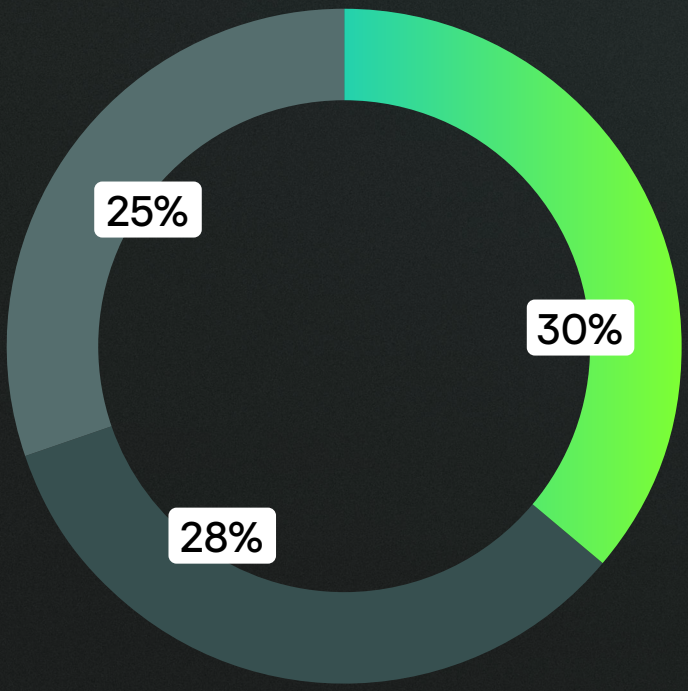
3 самые тяжелые темы для обсуждения с начальством[1]

- Необходимость увеличения бюджета ИБ-отдела
- Повышение осведомленности сотрудников о киберугрозах
- Расширение ИБ-отдела



3 главные причины урезания бюджетов ИБ в организациях[2]

- Бюджет службы безопасности перенаправляется на другие нужды компании
- «У нас достаточный уровень безопасности, нет смысла вкладывать дополнительные деньги в киберзащиту»
- Высшее руководство не понимает, зачем вкладываться в кибербезопасность



[1] Исследование Fluent in Infosec. «Лаборатория Касперского», 2023
[2] Managing the trend of growing IT complexity. «Лаборатория Касперского»

Вовлечение высшего руководства в вопросы кибербезопасности

Корпорации, где руководители активно участвуют в обсуждении и принятии решений по защите организации от киберугроз, лучше подготовлены к возможным атакам и способны оправиться от них быстрее и с меньшими потерями. Включенность совета директоров в эти вопросы позволяет обеспечить стабильный высокий уровень осведомленности в области кибербезопасности на всех уровнях работы организации. Но у высокого начальства, как правило, уже хватает других задач и очень плотный график. Как убедить их найти в нем время для обучения?

Ответом может стать тренинг, составленный с учетом потребностей высшего руководства, — специальная программа, призванная помочь руководству понять ландшафт киберугроз и его влияние на эффективность бизнеса, а также дать практические рекомендации по разработке и применению стратегий кибербезопасности, приносящих пользу всей компании.

Обучающая программа онлайн-курса

Курс разработан высшим руководством и ведущими специалистами по кибербезопасности «Лаборатории Касперского». Он состоит из 50 уроков длиной по 3–6 минут и доступен через облачную платформу или в формате SCORM для интеграции в корпоративную систему управления обучением (LMS). Эти программы входят в комплекс Kaspersky Security Awareness наряду со множеством других увлекательных обучающих решений, призванных повысить осведомленность ваших сотрудников и создать культуру кибербезопасности в организации.

Подробнее

Онлайн- и офлайн-тренинги по кибербезопасности для руководителей высшего звена

Повышение осведомленности топ-менеджеров в области кибербезопасности

Кибербезопасность — такой же важный фактор прибыльности компании, как управление проектами, финансовые инструменты и операционная эффективность. Этой идее мы уделяем особое внимание на тренинге для руководителей.

Этот тренинг помогает высшему руководству компании усвоить основы кибербезопасности под руководством инструктора. В результате руководство лучше разбирается в киберугрозах и способах защиты от них.

Что дает тренинг?

Программа курса освещает критические для бизнеса аспекты кибербезопасности понятным, не требующим технических знаний языком. Он делает наглядной окупаемость инвестиций в кибербезопасность и способствует диалогу и кооперации между отделами в случае возникновения угроз. Тренинг для руководителей доступен в двух форматах:

1

Тренинг для руководителей

Интерактивный мастер-класс, который специалист «Лаборатории Касперского» проводит очно

2

Кибербезопасность для руководителей онлайн

Дистанционный тренинг

Тренинг «Кибербезопасность для руководителей онлайн» освещает шесть тем:

Введение в кибербезопасность	• Что такое кибербезопасность • Зачем руководителю заниматься вопросами кибербезопасности • Подход Евгения Касперского: от киберзащиты до кибериммунитета
Киберриски организаций	• Потери бизнеса от кибератак • Подходы к управлению киберрисками и меры защиты • Примеры успехов и провалов в управлении киберрисками
Кибератаки и арсенал злоумышленников	• Инструменты злоумышленников: социальная инженерия, вредоносное ПО, эксплойты, черный рынок • Кибератаки: классификация, факторы успеха, целевые атаки, массовые атаки, утечки данных, как защититься
Защита руководителей и компаний от кибератак	• Цифровая гигиена для руководителей • Осведомленность сотрудников о кибербезопасности и как ее повышать • Кибербезопасность на разных ступенях развития компании • Аудит кибербезопасности и сервисы кибербезопасности
Устранение последствий кибератак	• Реагирование на кибератаку и ответные меры • План действий в кризисных ситуациях, связанных с кибератаками • Как сообщать об инцидентах
Киберзащита будущего	• Киберугрозы: статистика и векторы атаки • Четвертая промышленная революция и интернет вещей • Кибериммунитет

К каждой теме прилагается практическое задание из 5–10 вопросов для самопроверки и закрепления новых знаний. После окончания всех уроков и выполнения всех заданий необходимо пройти финальный тест. По его итогам вы получите сертификат о прохождении курса.

Главные преимущества

Легко освоить

Небольшие порции информации, практические задания и тесты — рецепт хорошо усвоенных знаний

Удобный формат

Онлайн-курс адаптирован для компьютера и мобильных устройств

Практические руководства и чек-листы

К курсу прилагаются готовые материалы по кибербезопасности, применимые в повседневной работе

Глубокое понимание потребностей руководства

Курс составляли топ-менеджеры «Лаборатории Касперского»

Результаты курса

По итогам курса менеджеры овладеют следующими навыками:

Находить общий язык со специалистами по ИБ и IT

Совместно с отделом IT и службой информационной безопасности разрабатывать план действий в кризисных ситуациях, связанных с кибербезопасностью

Грамотно планировать коммуникации в случае инцидента

Принимать стратегические решения на основе оценки киберрисков

Следовать правилам цифровой гигиены

Защищаться от киберугроз

Kaspersky Security Awareness

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее