



# Тренинги Kaspersky Security Awareness

# Тренинги по безопасности Kaspersky Security Awareness

## Эффективный способ защитить цифровое пространство всей организации

Более 80% всех киберинцидентов вызваны человеческим фактором. Чтобы уменьшить поверхность атаки и снизить число инцидентов, организациям необходимо формировать в коллективе культуру безопасного поведения в интернете. В то же время подобрать подходящие инструменты и методы для развития навыков кибербезопасного поведения непросто. Необходим современный курс, содержащий актуальные материалы и задействующий новейшие технологии в области тренингов по кибербезопасности для взрослых.

## Kaspersky Security Awareness – системный подход к тренингам в сфере IT-безопасности

### Люди как наиболее уязвимый элемент кибербезопасности

Решения в сфере кибербезопасности быстро совершенствуются и адаптируются к сложным угрозам, затрудняя работу киберпреступников, и они направляют свои усилия в сторону самого уязвимого элемента – человеческого фактора.

**52% руководителей высшего звена** считают, что сотрудники представляют наибольшую угрозу операционной безопасности\*

**51,4% сотрудников** готовы дать свой пароль коллегам или же вовсе делают это регулярно\*\*

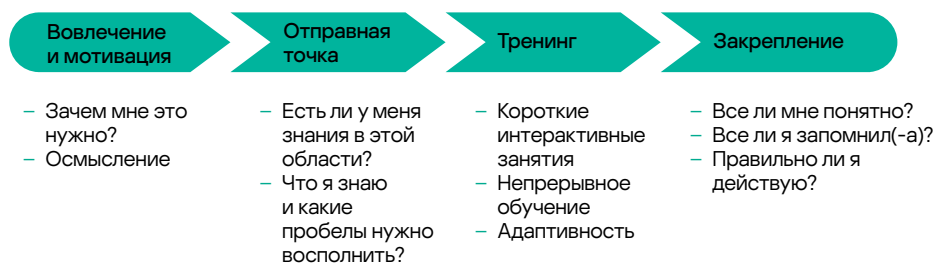
**67% сотрудников** используют рабочий компьютер в личных целях, а каждый 10 делит его с членами своей семьи\*\*

**23% организаций** не имеют правил или политик безопасности хранения корпоративных данных\*\*

**43% компаний** сегмента малого бизнеса пострадали от инцидентов безопасности, произошедших из-за нарушения сотрудниками политик IT-безопасности\*\*

Kaspersky Security Awareness предлагает ряд интересных и эффективных курсов для повышения осведомленности сотрудников и создания культуры кибербезопасности в организации. Поскольку для формирования устойчивых навыков безопасного поведения требуется время, наш подход подразумевает непрерывный и многокомпонентный цикл.

Цикл непрерывного получения знаний



### Ключевые особенности программы



#### Глубокие знания в области кибербезопасности

Более 20 лет опыта в этой сфере легли в основу наших тренингов



#### Тренинги, которые меняют поведение сотрудников на всех уровнях организации

Игровой формат тренингов помогает заинтересовать и мотивировать сотрудников, а упражнения позволяют закреплять полученные навыки

\* Независимый отчет "[Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure](#)".

\*\* Исследование Кода Дурова «[Кибербезопасность на работе](#)», октябрь, 2022.

# Мотивировать, а не принуждать

**Сотрудники совершают ошибки. Компании теряют деньги. Это можно исправить.**



**510 000 \$**

**(для крупных предприятий в РФ)**

составляет средний финансовый ущерб от киберинцидентов, вызванных неправильным использованием IT-ресурсов сотрудниками\*



**465 000 \$**

**(для крупных предприятий в РФ)**

составляет средний финансовый ущерб от утечек данных, вызванных несоблюдением внутренней ИБ политики\*



**86%**

**компаний**

сообщили, что по крайней мере один их сотрудник переходил по фишинговой ссылке\*\*



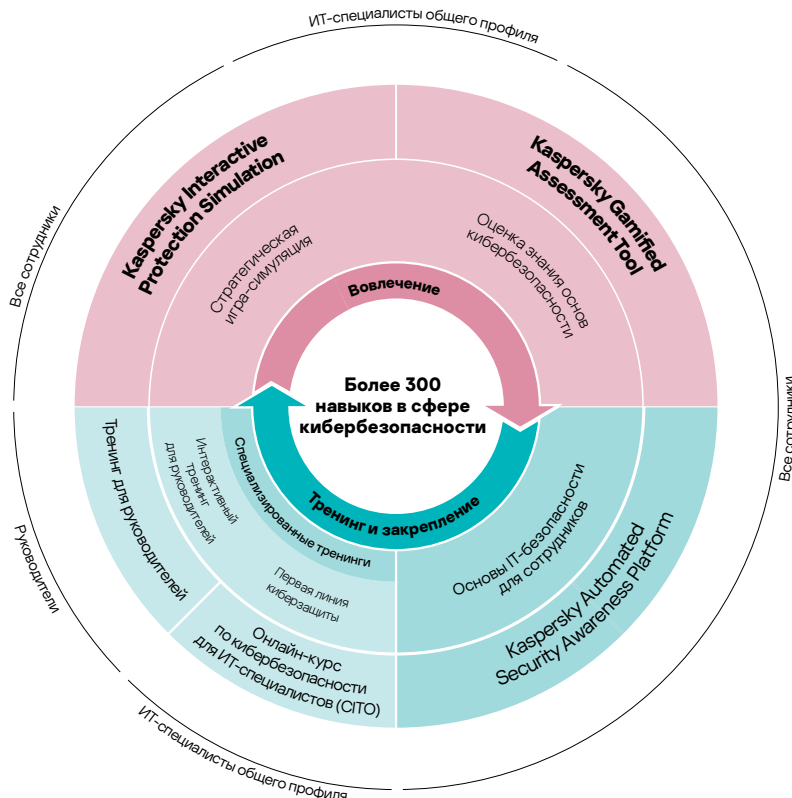
**62%**

**топ-менеджеров**

признали, что недопонимание с IT- или ИБ-отделом привело как минимум к одному инциденту в их организациях\*\*\*

Самая сложная задача в обучении кибербезопасности – изменить поведение сотрудников. Люди, как правило, не мотивированы получать новые навыки и менять свои привычки, из-за чего тренинг часто превращается в бесполезную формальность. Эффективное обучение должно состоять из различных компонентов, учитывать специфику человеческого мышления и способность усваивать полученные знания. «Лаборатория Касперского» знает, какое поведение пользователя можно считать безопасным. Мы совместили наш опыт с образовательными технологиями и методиками, чтобы сотрудники наших клиентов могли успешно проходить тренинги без давления со стороны руководства.

## Разные форматы тренингов для разных уровней организации



\* Отчет IT security economics in 2021 (Экономика IT-безопасности в 2021 г), «Лаборатория Касперского».

\*\* Отчет «Лаборатории Касперского» IT security economics in 2019 («Экономика IT-безопасности за 2019 год»).

\*\*\* Исследование «Лаборатории Касперского».

# Продукты Kaspersky Security Awareness



## Вовлечение и мотивация

Сотрудники не всегда настроены проходить дополнительные тренинги, а когда речь заходит о кибербезопасности, многие из них считают эту сферу слишком сложной или скучной, некоторые же уверены, что не имеют к ней никакого отношения. Без мотивации не стоит рассчитывать на положительные результаты. Еще одна непростая задача – вовлечь в процесс руководство компании, а ведь их ошибки могут обходиться компании столь же дорого, как и ошибки остальных сотрудников. В этом случае на помощь приходит игрофикация, самый эффективный способ заинтересовать сотрудников и преодолеть их сопротивление обучению на начальном этапе.

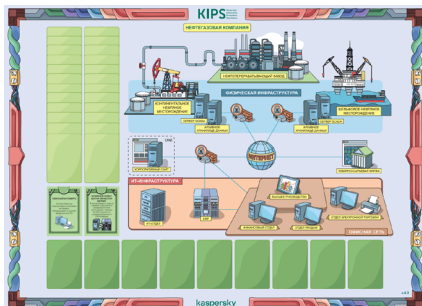
**До 60%** изученного материала

забывается в течение одного дня при традиционных формах обучения\*

**42% опрошенных, работающих в компаниях с более чем 1000 сотрудников,** сказали, что большинство обучающих программ, которые они проходили, оказались бесполезными и неинтересными\*\*

## Решение

**Тренинги Kaspersky Interactive Protection Simulation** предназначены для руководителей высшего звена, экспертов по бизнес-системам и сотрудников IT-отделов. Цель – повысить осведомленность о рисках и проблемах безопасности, связанных с современными компьютерными системами



## Стратегическая игра Kaspersky Interactive Protection Simulation: взгляд на кибербезопасность с точки зрения бизнеса

Kaspersky Interactive Protection Simulation – двухчасовая интерактивная командная игра, которая помогает наладить взаимопонимание между лицами, ответственными за принятие решений (руководителями бизнеса и специалистами по IT- и кибербезопасности), и изменяет их подход к обеспечению кибербезопасности в лучшую сторону. Она представляет собой программную симуляцию реального влияния вредоносного ПО и кибератак на производительность и доход компании. Игрокам необходимо мыслить стратегически, предугадывать последствия атаки и принимать соответствующие меры с учетом ограничений по времени и финансам. Каждое решение будет сказываться на всех бизнес-процессах, но работа компании не должна прерываться. Побеждает команда, которая закончила игру с наименьшими финансовыми потерями, нашла и проанализировала все бреши в системе кибербезопасности, а также приняла необходимые меры.

## Тринадцать отраслевых сценариев (регулярно добавляются новые)



Аэропорт



Корпорация



Банк



Нефтегазовая компания



Транспорт



Электростанция



ГЭС



Орган местного самоуправления



Нефтехимическое предприятие



Нефтяной холдинг



Малый и Средний бизнес



Телеком



Техническая атрибуция

Каждый сценарий демонстрирует участникам, насколько важна кибербезопасность для целостности и прибыльности бизнеса, учит определять новые проблемы и угрозы, а также показывает типичные ошибки в организации системы кибербезопасности. При этом коммерческий и ИБ-отделы взаимодействуют друг с другом, что помогает стабилизировать работу и противостоять киберугрозам.

## KIPS можно играть, как офлайн, так и онлайн.

KIPS офлайн очень популярен, так как сам формат очной командной игры создает непередаваемую атмосферу азарта и энтузиазма. Это отличный инструмент для вовлечения и создания культуры кибербезопасности внутри организации.

Онлайн-версия открывает перед пользователями, помимо очевидных – играть с большим количеством участников и из любого удобного места, другие возможности, связанные с персонализацией сценариев и возможностью получить статистику о выборе игроков, данные о действиях команд в тех или иных ситуациях, получить сравнение действий игроков по отношению к предыдущей игре.

## Персонализация сценариев

Новый улучшенный функционал игры позволяет персонализировать игровой сценарий, выбирая и комбинируя различные типы атак из библиотеки. Эта функциональность позволяет несколько раз играть в один и тот же отраслевой сценарий, поддерживая интерес игроков с помощью различных комбинаций атак.

\* Кривая Эббингауза (кривая забывания).

\*\* The digital talent gap («Нехватка талантов в цифровой индустрии»), Cargemini Consulting.





## Определение отправной точки

Люди, как правило, самостоятельно не могут оценить уровень своих знаний в области кибербезопасного поведения. Поэтому сначала необходимо пройти тестирование и получить развернутую оценку своих знаний и навыков в сфере кибербезопасности, чтобы выстроить эффективный процесс прохождения тренингов. Тестирование позволит не тратить время на изучение уже известного материала.



## Тренинг

Наша онлайн-платформа является основой программы по повышению осведомленности. Она содержит тренинги для отработки **более чем 300 навыков**, которые охватывают все основные направления в сфере кибербезопасности.

На каждом уроке разбираются конкретные ситуации и примеры из реальной жизни, с которыми сотрудники сталкиваются в своей повседневной работе. Такой подход позволит им применять полученные навыки уже после первого урока.

Kaspersky Automated Security Awareness Platform: удобный онлайн-инструмент, помогающий постепенно формировать у сотрудников навыки кибербезопасности.

### Темы Kaspersky Automated Security Awareness Platform:

- Пароли и учетные записи
- Безопасность электронной почты
- Работа в интернете
- Социальные сети и службы обмена сообщениями
- Безопасность компьютеров
- Мобильные устройства
- Защита конфиденциальных данных
- Персональные данные
- GDPR
- Кибербезопасность промышленных систем
- Безопасность банковских карт и PCI DSS
- Доксинг
- Безопасность криптовалют
- Информационная безопасность при работе из дома
- Ф3-152

### Экспресс-курс Kaspersky Automated Security Awareness Platform

Краткая версия тренинга в аудиовизуальном формате.

- Интерактивная теоретическая часть
- Видео
- Тесты

Kaspersky Automated Security Awareness Platform поддерживает несколько языков.

## Gamified Assessment Tool: быстрый и увлекательный способ оценить навыки сотрудников в области кибербезопасности

Инструмент оценки Kaspersky Gamified Assessment Tool позволяет провести анализ знаний сотрудников о безопасности в интернете. Всего за 15 минут сотрудникам необходимо проанализировать 12 жизненных ситуаций и оценить рискованность действий персонажа, указав степень своей уверенности в ответе.

В конце сотрудники получают сертификат с баллами, отражающими уровень осведомленности. Кроме того, они получают обратную связь с объяснениями и полезными советами по каждой ситуации.

С помощью игрового подхода Kaspersky Gamified Assessment Tool мотивирует сотрудников и выявляет имеющиеся у них заблуждения на примере конкретных ситуаций. Этот инструмент будет также полезен IT- и HR-отделам, чтобы оценить уровень осведомленности в сфере кибербезопасности у сотрудников своей организации. Такая оценка может служить первым шагом к развертыванию масштабной образовательной кампании.



## Kaspersky Automated Security Awareness Platform: онлайн-инструмент для развития практических навыков в сфере кибербезопасности

Kaspersky Automated Security Awareness Platform – простой и эффективный онлайн-инструмент, помогающий постепенно формировать у сотрудников навыки в сфере кибербезопасности и мотивировать их на правильное поведение.

Такое решение подойдет малому и среднему бизнесу, в особенности тем компаниям, у которых нет возможностей управлять тренингом.

### Ключевые преимущества решения

- **Простота благодаря полной автоматизации:** запускать, настраивать и контролировать программу легко, а управление полностью автоматизировано и не требует помощи администраторов. Платформа самостоятельно выстраивает план для каждой группы сотрудников, обеспечивая интервальное прохождение курса. Учащиеся постоянно закрепляют полученные знания благодаря различным форматам (в т. ч. обучающим модулям, электронным сообщениям с информацией и рекомендациями, тестам и имитациям фишинговых атак)
- **Эффективность:** материалы в программе структурированы так, чтобы обеспечивать последовательное интервальное прохождение тренинга с постоянным закреплением знаний. Методика учитывает особенности человеческой памяти: сотрудники лучше усваивают знания и смогут применять полученные навыки.
- **Разный формат:** вы можете выбрать программу, которая лучше всего отвечает потребностям сотрудников. Например, базовый экспресс-курс поможет освежить их знания, а основной курс, включающий несколько уровней сложности, подойдет для более глубокого освоения навыков кибербезопасного поведения.
- **Имитации фишинговых атак** можно проводить до, во время или после тренинга, чтобы проверить, хорошо ли сотрудники распознают киберугрозы. Имитации помогут оценить преимущества тренинга и самим сотрудникам, и руководству компании.
- **Гибкое лицензирование** (для поставщиков управляемых услуг): из расчета на одного пользователя (можно использовать, начиная с 5 лицензий).

Каждая тема делится на разные уровни, посвященные отработке определенной группы навыков в сфере безопасности. Уровни соответствуют степени опасности угроз. На первом уровне участникам объясняют, как себя вести при прямых и массовых атаках. Проходя уровень за уровнем, они переходят к изучению поведения при целевых атаках и сложных угрозах.

## Kaspersky Automated Security Awareness Platform для партнеров

Kaspersky ASAP идеально подходит для всех поставщиков услуг (в том числе услуг по управлению) – тренингом для различных бизнес-подразделений можно управлять из единой учетной записи. Лицензии можно приобретать по подписке с ежемесячной оплатой.

Попробуйте полнофункциональную версию Kaspersky Automated Security Awareness Platform. Ее можно найти на сайте [k-asap.ru](http://k-asap.ru).

## Интерактивные занятия

**ВОПРОС**  
Вы заходите в интернет-магазин еды и игрушки для домашних животных. Сервис просит вас зарегистрироваться и ввести свой адрес электронной почты в качестве логина, а пароль от почты — в качестве пароля от личного кабинета. Что делать?

Выберите вариант ответа и нажмите на кнопку «ОТВЕТИТЬ»:

Ввести пароль — это необходимое условие регистрации  
Не вводить пароль от почты, придумать новый  
Закрыть сайт — он явно мошеннический

Упражнение 2 из 2  
Попытайтесь установить пароль, даже если вы работаете дома.  
Ваша отправка должна быть безопасна, чтобы избежать фишинга или кражи данных.  
Как вы считаете, через какое время должна сработать блокировка экрана? Выберите один вариант ответа

## Имитация фишинговых атак

**С вашего счета сделан перевод в пользу клиента Inesobank**  
1 фишинг

Inesobank - email@inesobank.ru  
KSPY: rakabank@kaspersky.com

**INESOBANK**

Уважаемый Родион Раскольников, с вашего банковского счета была совершена следующая транзакция в пользу банка Inesobank

Получатель: Р. Р. Раскольников  
Идентификационный номер: 2063370371851701  
Количество: \$451.43  
На счет: Кареленя Зюльда Тимовича (2065293374501001)  
Сделка: Перевод в доллары США

Оспорить

+7 495 345 81 99 inesobank@inesobank.ru 17 | © 2018, Москва

## Отслеживание результатов

На информационной панели вы можете отслеживать результаты сотрудников и оценивать прогресс всех сотрудников и каждой группы. Также можно получить доступ к более подробной информации по отдельным сотрудникам.

## Симулированные фишинговые атаки

Фишинг по-прежнему входит в топ-3 причин киберинцидентов. Поэтому, помимо интерактивных уроков и тестов, важно закрепить навык распознавания фишинга на практике.

В автоматизированной платформе Kaspersky ASAP фишинг является как частью пути обучения в основном курсе, так и самостоятельным блоком. В первом случае от администратора обучением не требуется предпринимать никаких действий. Атака, соответствующая отработке пройденной темы, будет отправлена платформой автоматически.

Симулированную фишинговую кампанию можно запустить до, во время и в конце обучения для сравнения результатов и оценки прогресса.

- Более 120 редактируемых фишинговых шаблонов, которые постоянно обновляются и пополняются в соответствии с реальными угрозами;
- Возможность выбрать шаблоны и запустить разные симулированные атаки для разных групп сотрудников, исходя из данных о частоте провалов;
- Возможность проведения «слепой» фишинговой кампании, когда важно, чтобы сотрудники не догадались, что это учебная атака



**Закрепление** – неотъемлемая часть программы по повышению осведомленности, направленная на усвоение полученных знаний и навыков.

Лучший способ обратить полученные навыки в привычку – это применять их на практике. В то же время люди иногда совершают ошибки и учатся на личном опыте. Но когда дело касается кибербезопасности, обучение на собственных ошибках может обойтись слишком дорого.

Предоставить доступ к таблице?

k.n@support.io запрашивает доступ к следующей таблице:

Publication\_plan.xlsx

Открыть доступ Настройки доступа

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA  
Вы получили это электронное письмо, поскольку пользователь k.n@support.io запросил доступ к таблице Google

Помогите нам стать лучше!

Команда HR проводит исследование об удовлетворенности наших сотрудников текущими условиями работы и компенсационным пакетом.

Пожалуйста, пройдите небольшое исследование, которое позволит нам понять, пользуетесь ли вы всеми положенными вам льготами и компенсациями, а также улучшить наше предложение для вас.

Прохождение опроса займет 5-7 минут.

Пожалуйста, пройдите опрос до 31.12.2019

Ваше мнение важно для нас!

Пройти опрос



## Оптимальная программа для IT-специалистов

Большинство компаний внедряют тренинги на двух уровнях: повышают квалификацию сотрудников отдела IT-безопасности и учат основам кибербезопасности сотрудников, вообще не связанных с IT. Однако в этой картине не хватает важного элемента. Обучение не затрагивает IT-профессионалов, службу IT-поддержки и других технических сотрудников. Стандартных программ осведомленности для них недостаточно, при этом делать из технических специалистов полноценных экспертов по кибербезопасности за корпоративный счет слишком дорого и долго – другими словами, не нужно.

**Курс по кибербезопасности для корпоративных IT-специалистов (CISO)** проводится онлайн, участникам нужен лишь доступ в интернет и к системе управления обучением (LMS), а также браузер Chrome.

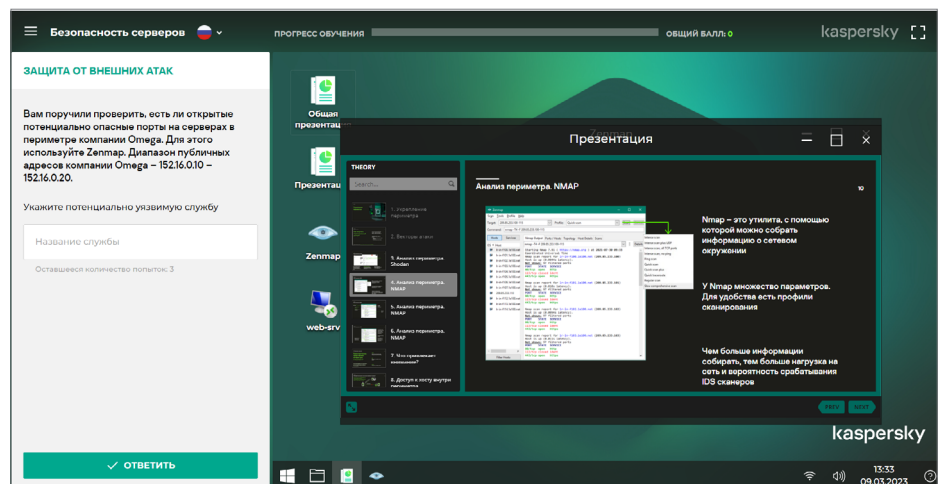
Каждый из 6 модулей состоит из короткой теоретической части, практических рекомендаций и 4–10 упражнений: каждое позволяет отработать определенный практический навык, а также учит использовать защитные инструменты и ПО в повседневной работе.

## Онлайн-курс по кибербезопасности для IT-специалистов (CISO): первая линия киберобороны

Это интерактивный курс для всех IT-специалистов. Он позволяет сформировать профессиональные навыки по обеспечению кибербезопасности и реагированию на инциденты первого уровня.

Курс предназначен специально для IT-специалистов и учитывает их высокий уровень технической осведомленности и специфику рабочих обязанностей. Кроме того, тренинг мотивирует IT-специалистов искать признаки кибератаки и помогает понять, что они должны делать на первой линии киберобороны. Тренинг также формирует базовые знания о расследовании угроз и использовании защитных инструментов и программ. IT-специалисты обретают теоретические знания и практические навыки, закрепляя их упражнениями. Они также учатся собирать данные инцидентов безопасности и передавать их сотрудникам службы информационной безопасности.

Мы рекомендуем этот курс всем IT-специалистам в организации, особенно работникам службы IT-поддержки и системным администраторам. Также он будет полезен и специалистам других отделов – в частности, всем, кто имеет права локального администратора на своей рабочей станции.



## Тренинг для руководителей: повышение устойчивости бизнеса в эпоху цифровой трансформации

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

Исследования выявили прямую связь между скоростью и эффективностью реагирования на инциденты и степенью ущерба от них. Особое внимание уделяется финансовым аспектам кибербезопасности. Тренинг поможет руководству компании лучше понять связь между кибербезопасностью и эффективностью бизнеса и оценить целесообразность инвестирования в защиту.

Опционально Kaspersky Interactive Protection Simulation может дополнить тренинг для руководителей, чтобы закрепить полученные навыки в практических упражнениях.

### Цели курса

- Предоставить актуальную информацию о современных киберугрозах и связанных с ними рисках для бизнеса
- Ознакомить участников с современным ландшафтом угроз
- Предоставить возможность на практике отработать базовые корпоративные и индивидуальные правила кибербезопасности
- Проинформировать об основных требованиях в области кибербезопасности и их влиянии на бизнес
- Разъяснить основные понятия кибербезопасности и методы защиты от целевых атак
- Дать практические рекомендации по разработке корпоративной политики
- Проинформировать об особенностях коммуникаций при реагировании на инциденты и их расследовании

# Kaspersky Security Awareness: гибкий подход к формированию навыков кибербезопасного поведения

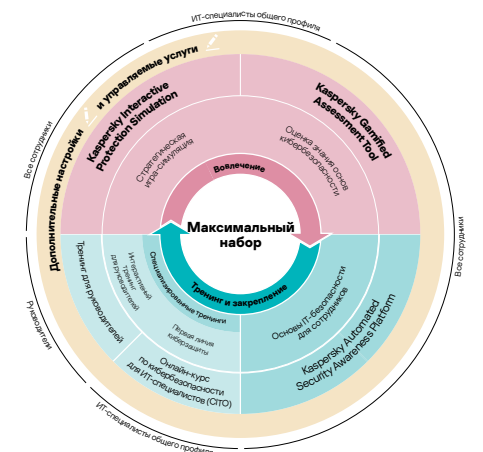
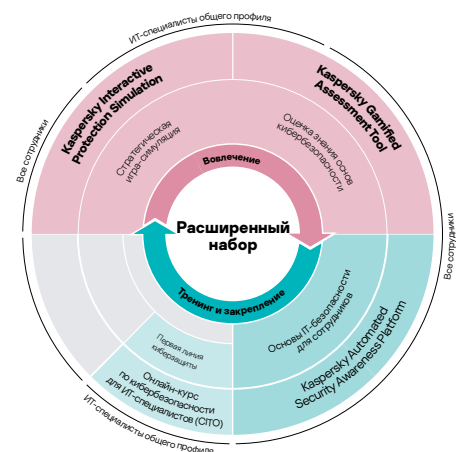
Выберите один тренинг для решения конкретной задачи безопасности или приобретите пакет тренингов, которые можно адаптировать под ваши потребности и приоритеты.

Базовый набор тренингов для повышения осведомленности сотрудников о киберугрозах – простой в установке и управлении.

Сотрудники получают базовые знания в области кибербезопасности, что поможет защитить компанию от угроз, связанных с человеческим фактором.

Расширенный набор тренингов для более крупных организаций, которым необходимо комплексное решение. Тренинги охватывают полный цикл получения знаний и помогут сформировать культуру кибербезопасности на всех уровнях организации.

Максимальный набор тренингов подойдет крупным предприятиям и государственным организациям. Включает персонализацию тренингов и доступ к управляемым услугам. Помогает руководителям компании понять сценарии атак, сотрудникам – усвоить навыки кибербезопасности, а ИТ-специалистам широкого профиля – сформировать навыки удержания первой линии киберобороны.



Подробная информация о пакетах тренингов на сайте: [kaspersky.ru/awareness](https://kaspersky.ru/awareness).

Kaspersky Security Awareness:  
[kaspersky.ru/awareness](https://kaspersky.ru/awareness)  
Попробовать Kaspersky ASAP  
[k-asap.ru](https://k-asap.ru)  
Новости ИТ-безопасности:  
[kaspersky.ru/blog/category/business](https://kaspersky.ru/blog/category/business)

[www.kaspersky.ru](https://www.kaspersky.ru)

**kaspersky** АКТИВИРУЙ  
БУДУЩЕЕ