Главная проблема российского бизнеса в области кибербезопасности — законы без стандартов

Издание: Mail.Ru Cloud Solutions, 8 мая 2019 г.

Спикер: Сергей Трещалин, руководитель направления развития услуг «Информзащиты»

В известных мировых рейтингах по информационной безопасности Россия занимает не самые лучшие места. Проблема в отсутствии рабочих ИБ-стандартов для организаций и, соответственно, в отсутствии культуры и грамотной корпоративной защиты. При этом отечественное законодательство оценивается как совершенное. Движение к стандартизации начал финсектор, рождаются реальные требования, инструкции и методики. Есть надежда, что успешная практика превратится в межотраслевые стандарты и будет принята бизнесом на вооружение.

У России всеохватывающее законодательство в области информационной безопасности (ИБ) — за период с начала нулевых разработана национальная стратегия в области ИБ и выпущены законы, регламентирующие все: от защиты персональных данных до ведения информационной войны. Тем не менее страна находится всего лишь на 38 месте по уровню информационной безопасности в целом. Так гласит рейтинг аналитической компании Comparitech, который объединяет оценки известных профильных рейтингов и рэнкингов. В чем причины низкого показателя?

Безопасность Шрёдингера

Рейтинг, выпущенный Comparitech, ранжирует все страны мира по уровню информационной безопасности. Места в рейтинге присваивались по сумме баллов за различные аспекты. Посмотрим на результаты, которые приписывают России.

Рейтинг	Страна	Баллы	Процент зараженных мобильных устройств	Финансовые вирусные атаки (% жертв)	Процент зараженных компьютеров	Процент атак на IoT из страны	Процент заражения вирусами для криптомайнинга	Уровень готовности к кибератакам	Законы в области ИБ
38	Russia	28.02	10.11	0.6	23	7.87	6.89	0.788	7

Источник: Comparitech, 2019

С одной стороны, Россия как бы и попадает во второй сегмент наиболее безопасных стран (между номером 25 и номером 40 в списке наименее защищенных).

С другой — общая сумма баллов по уязвимости к киберугрозам достаточно велика (у самых безопасных стран — Японии, Франции, Канады, Дании и США их от 8 до 12, у России — 28).

Гладко только на бумаге

Россия получила высшую оценку по уровню завершенности законодательства в области информационной безопасности. Такой вывод был сделан Comparitech на основе глобального рейтинга Cyber Regulation Index, который выпускается Центром стратегических и международных исследований США (CSIS).
Согласно рейтингу, в период с начала нулевых в России были разработаны законы, которые покрывают все семь категорий, необходимых для того, чтобы законодательство по ИБ считалось завершенным:

- Национальная стратегия по информационной безопасности;
- оборона государства в киберпространстве;
- ограничение доступа к определенному контенту;
- защита персональных данных пользователей;
- информационная защита критически важных объектов инфраструктуры;
- электронная коммерция и предоставление услуг интернет-сервисами;
- борьба с киберпреступностью.

СТРАНА	КАТЕГОРИЯ ЗАКОНОДАТЕЛЬСТВА						
	Стратегия	*Оборона*	*Контент*	*Перс. данные*	*Критически важные объекты*	*Коммерция*	*Борьба с преступностью*
Россия	2011, 2013	2014, 2015	2012	2006, 2014	2013, 2014	2006	1996, 2005

Источник: CSIS, 2019

Россия имеет одну из самых высоких оценок в рейтинге Comparitech по уровню готовности к кибератакам — 0,788. Более высокие результаты показывают только США, Канада, Австралия, Франция, Япония и Сингапур. Эта оценка основывается на глобальном рейтинге Global Cybersecurity Index 2017, который ежегодно выпускается Международным союзом электросвязи (МЭС). А Союз по итогам 2017 года включил Россию в топ-10 стран, наиболее защищенных от киберугроз извне.

Но влияет ли совершенное законодательство на реальную безопасность пользователей и организаций, которые живут и работают в стране? Эксперты считают, что не очень. Приводит пример **Сергей Трещалин**, руководитель направления развития услуг компании «Информзащита»: «Скажем, закон о персональных данных – он есть, но в нем много формализма и неудобств, связанных с необходимостью постоянно раздавать согласия на обработку своих персональных данных, в которых, зачастую, содержится и согласие на передачу их всему миру. Аналогичный пример в Европе: там обеспечение соответствия требованиям так называемого стандарта GDPR по обработке персональных данных для многих небольших организаций просто непосильно: в денежном исчислении необходимые затраты превышают годовую прибыль. Поэтому к данному вопросу компании подходят очень осторожно и взвешенно».

Если заглянуть в рейтинг МЭС, то становится ясно, в каких практических аспектах госрегулирования информационной безопасности Россия «проседает»:

Рис. 6.5.2. Оценка безопасности в странах СНГ

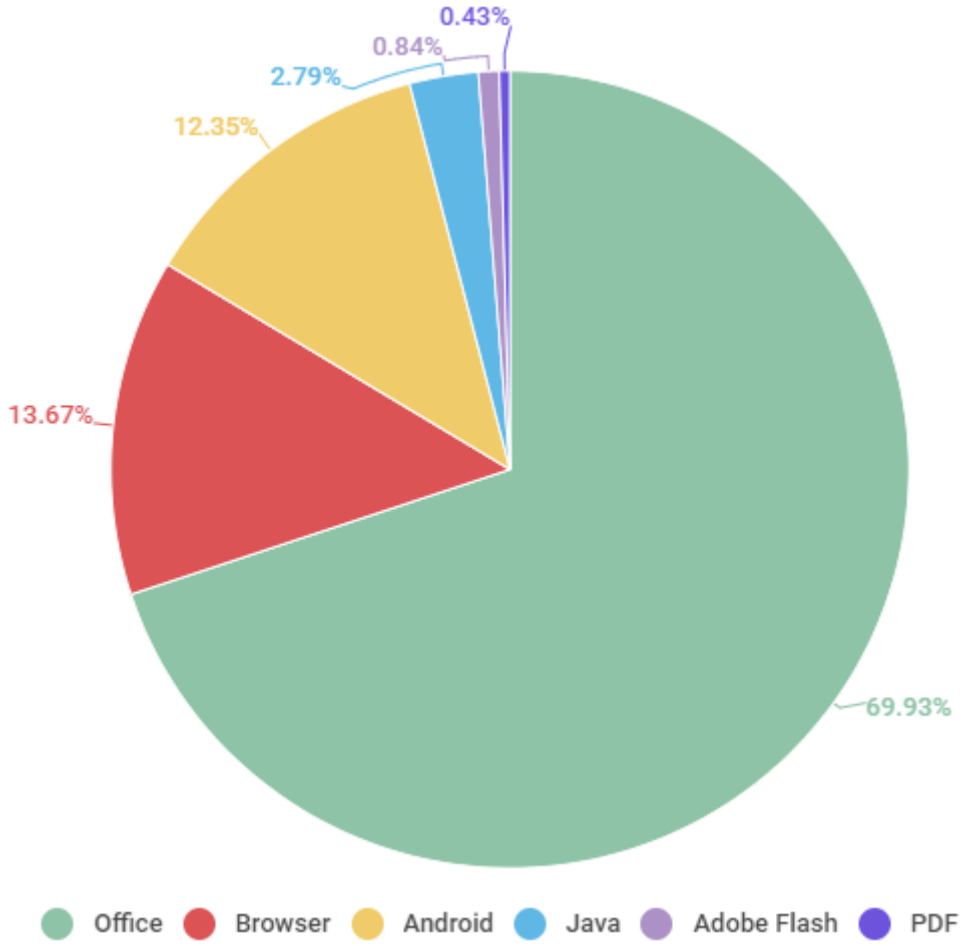
Источник: МЭС, 2017

С большинством из них сложно не согласиться. К примеру, отсутствие международных соглашений по ИБ и соответствующих указаний в законодательстве о борьбе с киберпреступностью значительно эту борьбу тормозят. «Мне кажется, тут следует говорить не об отдельных мерах, а об организации глобального взаимодействия в сфере борьбы с киберпреступлениями, — рассказывает Сергей Трещалин. — Основная сложность – в трансграничности. Для того чтобы атаковать российские компании, преступники нанимают сервера в Европе или Африке и работают через них. Любое расследование тут же упирается в кучу непреодолимых бюрократических процедур, что не позволяет оперативно выявлять злоумышленников». Конечно, проблема характерна не только для России.

Бизнесу нужны стандарты

Если еще раз взглянуть на таблицу МЭС, становится очевидно, в чем Россия отстает сильнее всего — это наличие стандартов информационной безопасности для организаций. «Красная метка» означает, что они не то что находятся в зародыше, а отсутствуют вовсе. В стадии разработки пока находятся и единые стандарты работы специалистов по безопасности, которые обслуживают организации.
Между тем, Comparitech отмечает, что в России достаточно большой процент атак на ПК (23%). Цифра позаимствована из отчета «Лаборатории Касперского» (ЛК) IT Threat Evolution за третий квартал 2018 года. Вендор называет основной источник заражения компьютеров вредоносным ПО. Им оказывается один из главных инструментов бизнеса — MS Office. Процент атак на офис в пять раз выше, даже чем у веб-браузеров, второй целевой платформы для хакеров.

Источники заражения компьютеров вредоносным ПО



Источник: «Лаборатория Касперского», 2018

Все это указывает на серьезную проблему при организации защиты информации в российском бизнесе. В условиях отсутствия единых стандартов ИБ в организациях каждая фирма «держит оборону» так, как умеет, утверждают эксперты. «Компании при построении ИБ руководствуются собственным опытом и общими требованиями ключевых регуляторов. Они часто не решаются на какие-то оригинальные действия. Хорошим примером является сдержанная позиция финансовых организаций по «уходу в облака» в ожидании официального мнения регулятора», — рассказывает **Сергей Терехов**, директор Центра компетенций по информационной безопасности компании «Техносерв».

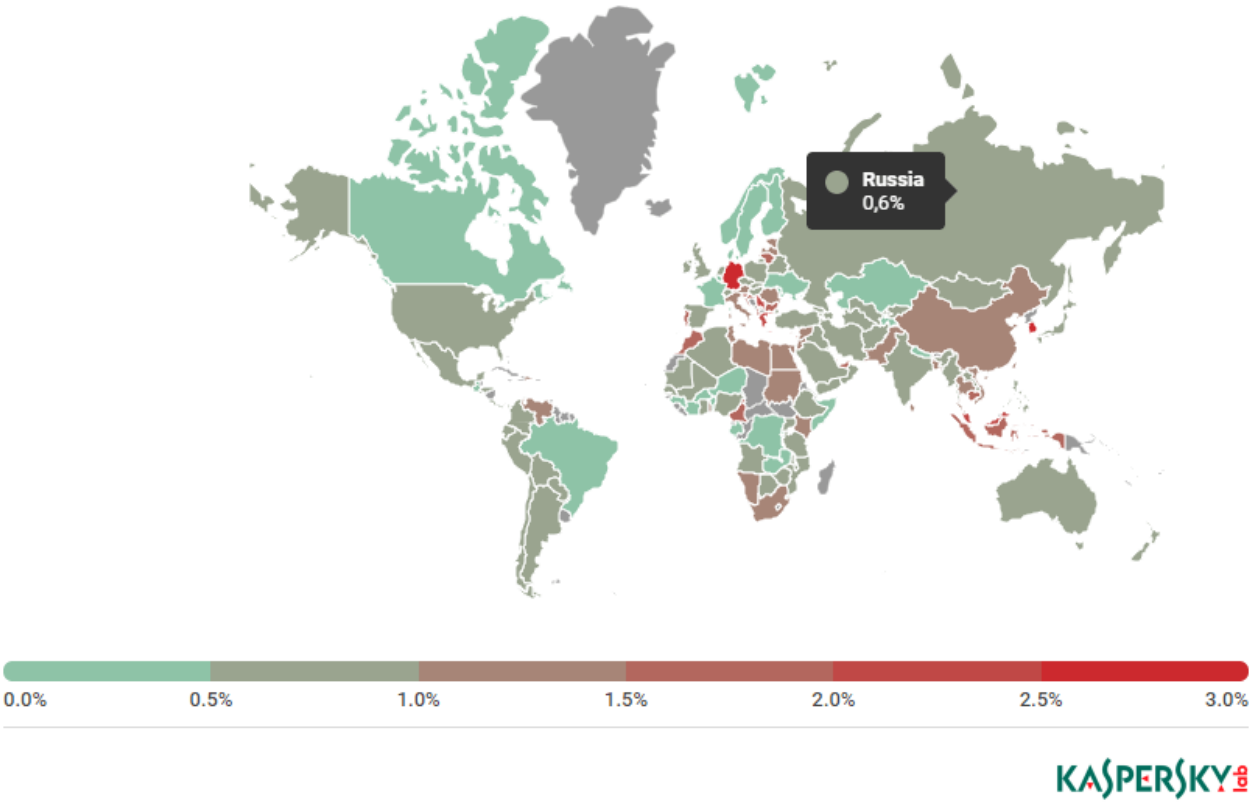
Банки начинают и выигрывают

Стандартизация ИБ для бизнеса в России только начинается. «Застрельщиком» выступает финансовый сектор, который традиционно является наиболее привлекательной мишенью для хакеров. Разработкой стандартов организации защиты для российских банков занимается основной регулятор — Центробанк РФ.
Кроме того, большой положительный эффект возымело принятие закона о защите критически важных объектов инфраструктуры — его обновленная версия появилась в 2017 году. Благодаря этому был создан центр оперативного реагирования на угрозы ГосСОПКА, указания которого должны стать практическим стандартом для КИИ (критической информационной инфраструктуры).

«Ключевым положительным моментом в России по части нормативного регулирования является постепенное смещение акцентов от «бумажной» безопасности в сторону «реальной». Поэтому когда мы сегодня говорим о том, что защита организаций соответствует законодательству, это действительно достаточно высокий уровень безопасности», — объясняет Сергей Терехов.

В первую очередь это относится к нормативной деятельности ЦБ РФ последних лет и законодательству о безопасности КИИ РФ, в частности деятельности ФинЦЕРТ и ГосСОПКА. Большинство компаний – владельцев объектов КИИ уже приводят их в соответствие законодательству собственными силами или с привлечением экспертных организаций, рассказывает Сергей Терехов. Многие организации внедряют у себя Security Operations Center (SOC) и организуют операционную деятельность по мониторингу, предотвращению и реагированию на инциденты ИБ. И если ранее проверка по линии, например, защиты персональных данных, проходила в форме изучения представителем регулятора стопок документации, то сегодня применяются техники тестирования на проникновение для проверки реального уровня защищенности. «Немаловажным моментом является общая тенденция к ужесточению ответственности для бизнеса в случае инцидентов ИБ, например в части уголовной ответственности или потенциальных рисков отзыва банковской лицензии», — считает эксперт.
Действительно, уровень атак вредоносного ПО на банковский сектор (к примеру, на банкоматы и платежные терминалы) в 2018 году крайне невысок — пристальное внимание регулятора к безопасности не могло не сказаться. Comparitech называет цифру в 0,6%, которая приводится в том же отчете «Лаборатории Касперского».

Уровень атак вредоносного ПО на банковский сектор в России в 2018 году

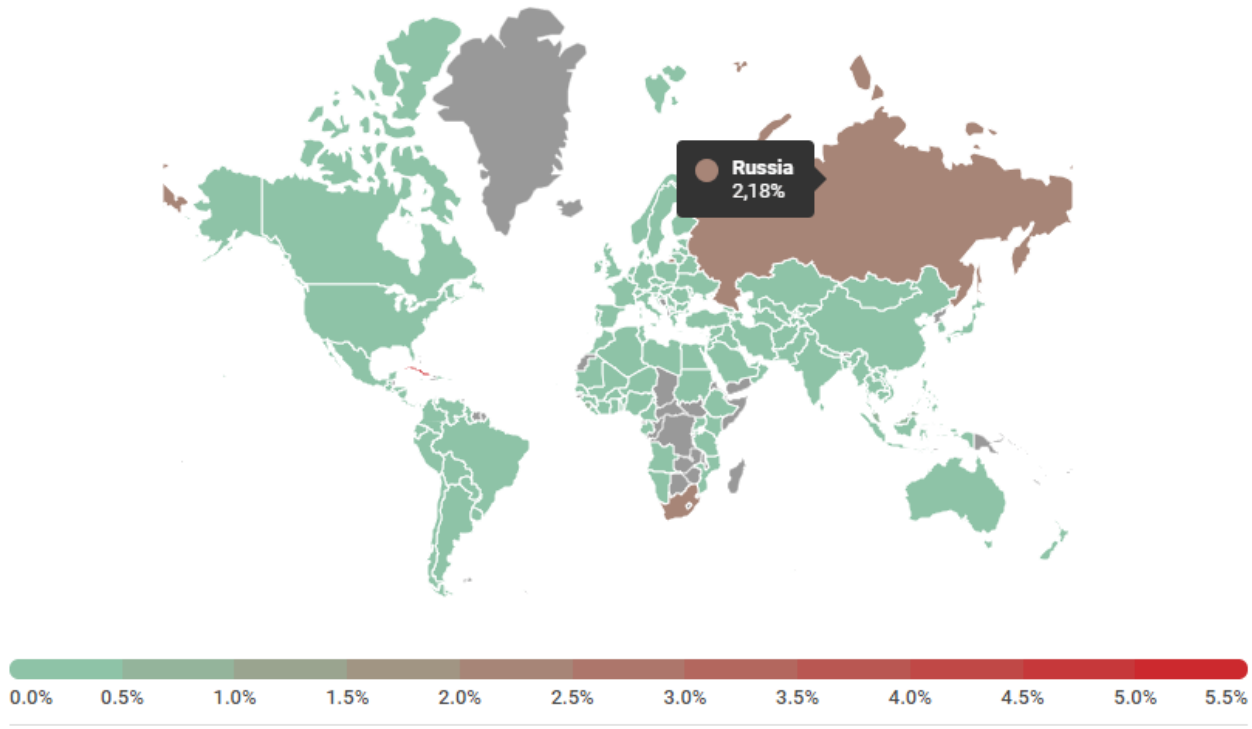


Компания «Информзащита»
Тел.: +7 (495) 980-2345
E-mail: pr@infosec.ru

Главная угроза — перед монитором

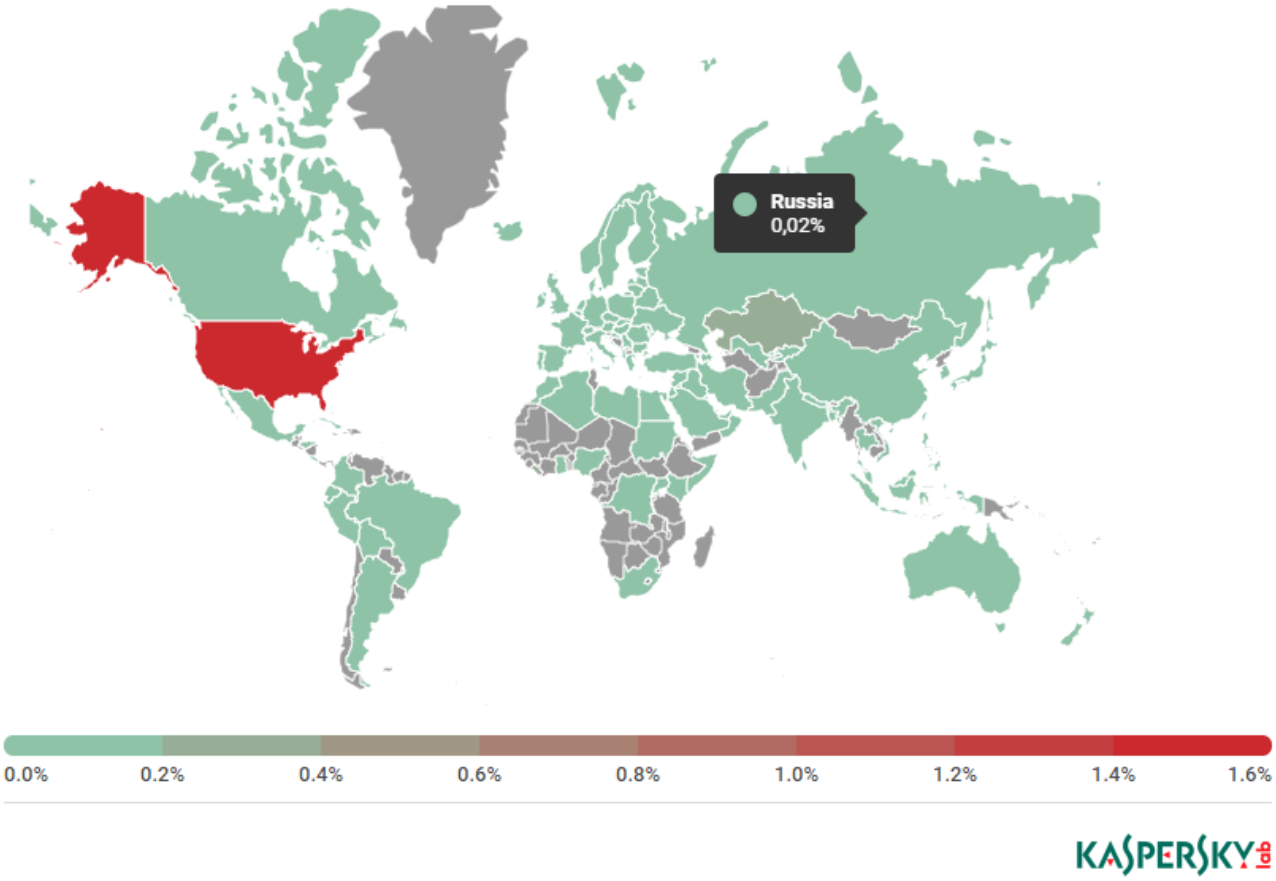
Чего же бизнесу следует опасаться в условиях, когда стандарты ИБ еще в разработке? Как показывает практика — собственных сотрудников. Приведенная статистика по заражению локальных компьютеров показывает, что основная угроза безопасности компаний — недостаточная информированность или халатность пользователей. Ведь именно они открывают присланные по электронной почте ссылки или зараженные документы Office.
А уровень информированности пользователей о защите от киберугроз довольно низок, о чем свидетельствуют собранные ЛК данные по заражению мобильных устройств — вещей сугубо индивидуальных, не подчиняющихся корпоративной политике. Согласно Kaspersky Labs и Comparitech, общее число зараженных мобильных устройств в России составляет 10,11% — что довольно мало в сравнении с другими странами. При этом в стране достаточно высокий процент зараженности вирусами-криптомайнерами (6,78%). Лаборатория Касперского в своем отчете еще приводит статистику по заражению мобильными вирусами, нацеленными на интернет-банки. С такими угрозами российские пользователи сталкиваются чаще, чем в среднем жители других стран.

Уровень заражения мобильными вирусами, нацеленными на интернет-банки, в России



Такая разница в цифрах (зараженных устройств мало, но заражений много) свидетельствует о неинформированности пользователей об актуальных угрозах. Чтобы было понятнее, по статистике Kaspersky Labs, в России низкий уровень заражения вирусами, гремевшими по всему миру в 2017 году — вирусами-вымогателями и шифровальщиками.

Уровень заражения вирусами-вымогателями и шифровальщиками в России



Когда до России докатилась волна эпидемии вирусов-шифровальщиков WannaCry и Petya, в стране прошла широкомасштабная кампания по освещению и предупреждению угрозы — на уровне государства, СМИ и корпораций. Таким образом, о зловредах-вымогателях российский пользователь в 2018 году знает — его проинформировали в предыдущем.
А вот о новых угрозах 2018 года — будь то вирусах-криптомайнерах или, к примеру, трояне Asacub, атакующем мобильные банки — говорят пока только специалисты по ИБ. Обычный пользователь не в курсе, так как информирование об актуальных угрозах у нас запаздывает в среднем на год, говорит Сергей Трещалин. В такой ситуации бизнесу следует задуматься о том, чтобы взять информирование сотрудников на себя. «Человек был, есть и будет самым слабым звеном в безопасности, — комментирует эксперт. — Даже на самые защищенные объекты можно проникнуть благодаря глупости, халатности или умыслу персонала. Оператору химического производства скучно дежурить ночью – он приносит USB модем или подключает к станции управления телефон с целью скоротать время за любимым сериалом, «выставляя» при этом систему управления производством в интернет».

Формирование культуры информационной безопасности – один из самых важных и наиболее труднодостижимых аспектов ИБ, добавляет Сергей Терехов. В деятельности подразделения информационной безопасности остальные – от бухгалтерии до программистов и ИТ – часто видят препятствия. Поэтому необходим локомотив развития культуры ИБ.

Ну не увольнять же?

Как бороться с неграмотностью пользователей — мнения экспертов расходятся. Одни считают эффективной политику ограничения пользователей в правах, другие — обучение и внушение. Так, **Игорь Корчагин**, руководитель группы обеспечения безопасности информации компании ИВК, считает, что во главе угла должны стоять технические меры: «Исключить или существенно сократить число неумышленных нарушений безопасности сотрудниками помогает четко продуманная и реализованная политика информационной безопасности. Корпоративная система ИБ должна быть выстроена таким образом, чтобы получать максимум сведений о различной активности пользователей. Например, жесткая система контроля использования отчуждаемых носителей, вплоть до запрета, существенно снижает реализацию угроз от случайной утери таких носителей».

Другой эксперт считает, что нужно не запрещать, а обучать и повышать осознанность. «Локомотивом развития культуры ИБ» должен выступать центр оперативного реагирования на киберугрозы (SOC), аналогичный государственным ФинЦЕРТ (Центр кибербезопасности ЦБ РФ) и ГосСОПКА (для КИИ, соответственно). Если его нет на уровне отрасли, его можно создать на уровне корпорации, полагает **Сергей Терехов**: «Для просвещения сотрудников необходимо, прежде всего, наладить операционные процессы информационной безопасности. В компании должны быть разработаны playbook'и (инструкция, как реагировать пользователям, руководству, службе информационной безопасности — прим. Mail.Ru Cloud Solutions) на каждую актуальную киберугрозу, организован процесс взаимодействия персонала различных подразделений в отношении реагирования на инциденты ИБ. Помимо этого, в компании должны регулярно проводиться мероприятия по повышению уровня культуры информационной безопасности за счет постоянного обучения и контроля осведомленности сотрудников в вопросах ИБ».

Скептики могут заметить, что позволить себе целый отдел, занимающийся «учениями по ИБ», может разве что крупный бизнес. Средним и малым компаниям, скорее всего, придется отдавать информирование пользователей на аутсорсинг — к примеру, путем заключения договора с интегратором решений ИБ.

В любом случае, одним развитым законодательством тут не обойтись. Нужны практические указания центров по стандартизации, которые позволят российскому бизнесу эффективно поднимать осознанность пользователей в вопросах ИБ. «Бороться можно лишь с помощью регулярного просвещения сотрудников в вопросах кибергигиены. А за нарушения предписанных правил поведения – обязательно наказывать, — подводит итог Сергей Трещалин. — Наш опыт подсказывает, что даже простые тренинги персонала в вопросах ИБ помогут значительно снизить угрозу от атак, направленных на организацию».

Подробнее: https://mcs.mail.ru/blog/sotrudniki-rossijskih-kompanij-nedostatochno-informirovany-o-kiberugrozah/