«АКТИОН» Образование

Как поддерживать информационную безопасность организации и отдельных граждан

Главное правило. Безопасное удобным не бывает.

Строго выполнять инструкции по защите информации. Например, не отключать антивирус, не использовать посторонние флеш-накопители на аттестованном персональном компьютере. Каждое из правил опирается на опыт специалистов. Пренебрежение безопасностью в угоду удобству обязательно приведет к инциденту.

Регулярно обучать работников. Знакомить с правилами информационной безопасности, оповещать о новых угрозах или видах мошенничества. С новыми видами угроз и методами противодействия можно ознакомиться на сайтах крупных производителей средств защиты информации: Касперский, Positive Technologies, Сёрчинформ, а также на официальных сайтах органов государственной власти, например, МВД или Роскомнадзора.

Создать чат для оповещения родителей, в котором публиковать может только администратор чата. Безопасных мессенджеров не существует, информация о том, что какой-то мессенджер гарантирует защиту от всех угроз, – это миф. Массовые чаты по разным вопросам – удобный источник для сбора информации злоумышленниками и для распространения фишинговых ссылок или вредоносного программного обеспечения.

Не собирать какие-либо данные через веб-формы. В крайнем случае с минимальным набором персональных данных для идентификации (например, только Фамилию И. О.).