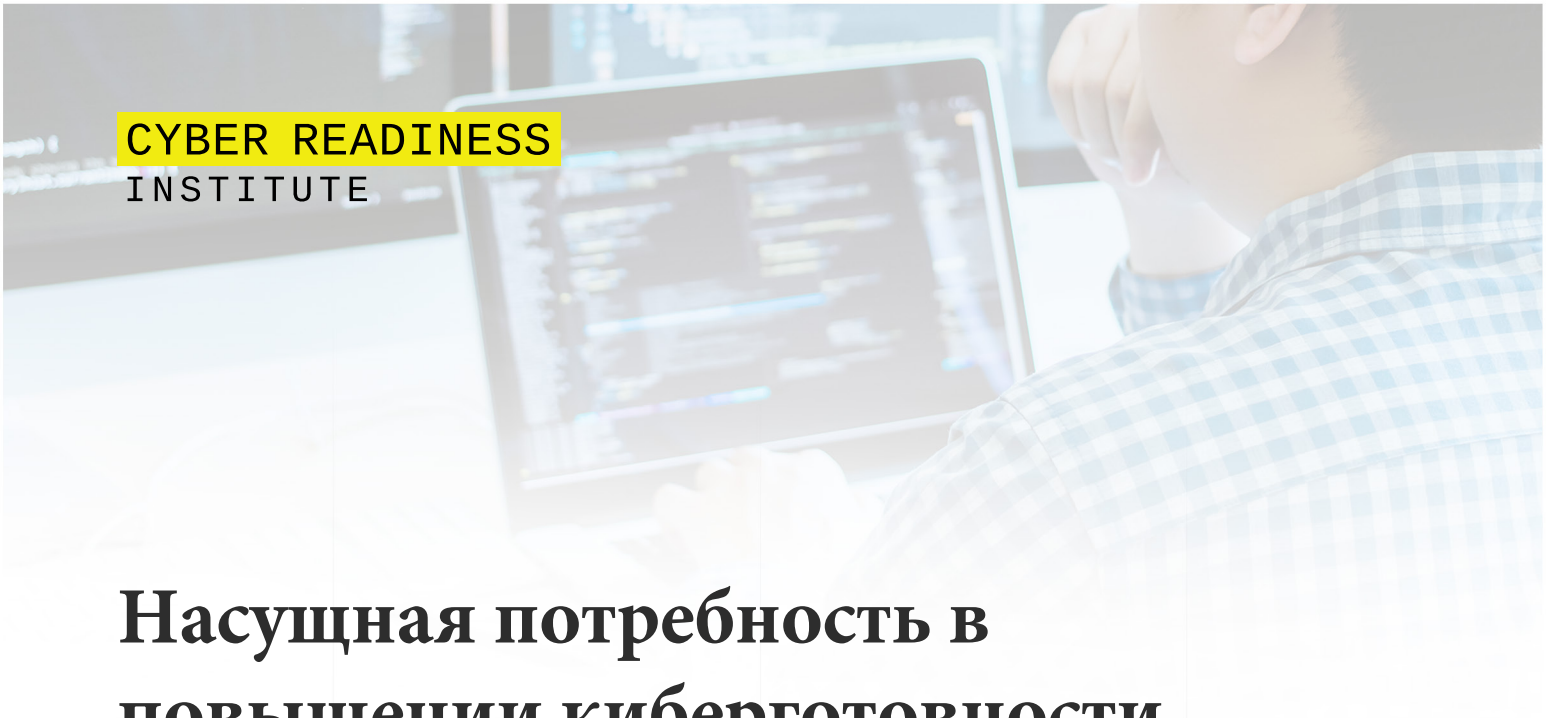


CYBER READINESS
INSTITUTE

Насущная потребность в повышении киберготовности малых и средних предприятий

Предложение для администрации Байдена

«По мере того, как мир все больше погружается в информационную революцию и становится зависимым от нее, темпы вторжений, сбоев, манипуляций и краж также ускоряются. Технологический прогресс опережает безопасность и будет продолжать делать это, если мы не изменим наш подход и внедрение стратегий и методов кибербезопасности. Недавние атаки, в ходе которых персональные устройства были скомпрометированы с целью злонамеренного использования, совершенно ясно показали, что теперь мы живем в гораздо более взаимозависимом мире».

- Комиссия по повышению национальной кибербезопасности, Отчет о безопасности и развитии цифровой экономики, 1 декабря 2016 г.

Спустя почти пять лет эти слова по-прежнему звучат правдоподобно. Мы по-прежнему погрязли в кошмарной игре «Ударь крота» с нашими киберпротивниками. Но сейчас цифровой ландшафт стал больше, и мы понятия не имеем, где появится следующая кибератака. Что мы знаем с уверенностью, так это то, что она произойдет. Обнаружение основных действий злоумышленников посредством компрометации SolarWinds и Microsoft Exchange произошло тогда, когда мы вышли из пандемического года удаленных бизнес-операций, когда наблюдался резкий рост атак программ-вымогателей на больницы, школы и другую критически важную инфраструктуру. Мы находимся в переломном моменте, и необходимо действовать срочно.

info@cyberreadinessinstitute.org

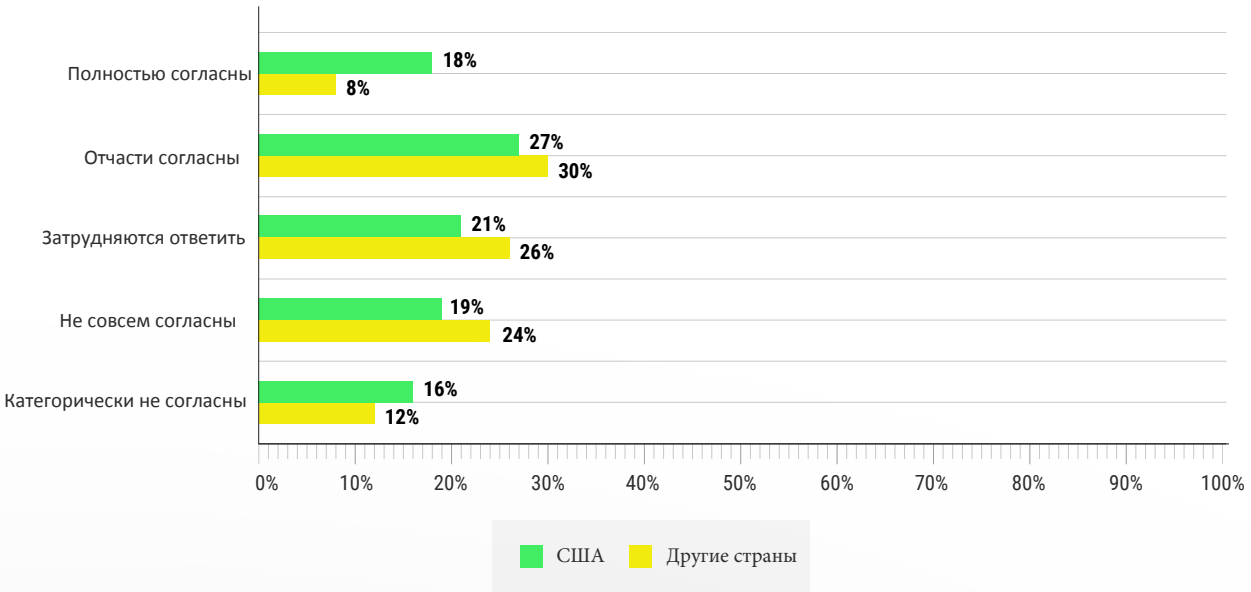
Невероятно обширные и изощренные события SolarWinds и Microsoft Exchange были лишь симптомами проблем, с которыми мы сталкиваемся. Усилий по исправлению положения таких, как обновление и исправление нашего программного обеспечения, изменение паролей и удаление вредоносного кода, недостаточно. Мы должны признать и устранить нашу неспособность стимулировать безопасное поведение и принять меры, необходимые для укрепления нашей киберзащиты, чтобы сделать нашу страну кибербезопасной.

События SolarWinds и Microsoft Exchange поставили под угрозу десятки малых и средних предприятий (МСП), которые образуют жизненно важные звенья в цепочках поставок и экономике нашей страны. Малые и средние предприятия становятся мишенью для кибератак, так как им часто не хватает ресурсов для инвестиций в инструменты и обучение кибербезопасности. Цель этой Белой книги — предоставить администрации Байдена конкретные действия по повышению устойчивости и киберготовности малых и средних предприятий США.

Хотя мы не можем положить конец кибервторжениям, есть основные действия, которые мы можем предпринять, чтобы защитить наших граждан, предприятия и критически важную инфраструктуру. Сосредоточив внимание на роли, которую поведение человека играет в успешных взломах, и предоставив малым и средним предприятиям инструменты и ресурсы для повышения их киберготовности, мы можем создать прочную и устойчивую основу для кибербезопасности.

Мы также можем помочь укрепить бизнес и выжить ему. Учитывая то, что 60% предприятий малого и среднего бизнеса закроются в течение одного года после кибератаки, по данным Национального альянса кибербезопасности, для малого и среднего бизнеса и для всех нас жизненно важно, чтобы они были осведомлены о кибербезопасности и готовы к ней.

Только 18% малых и средних предприятий США уверены в том («полностью согласны с тем»), что их организация готова к киберинциденту.



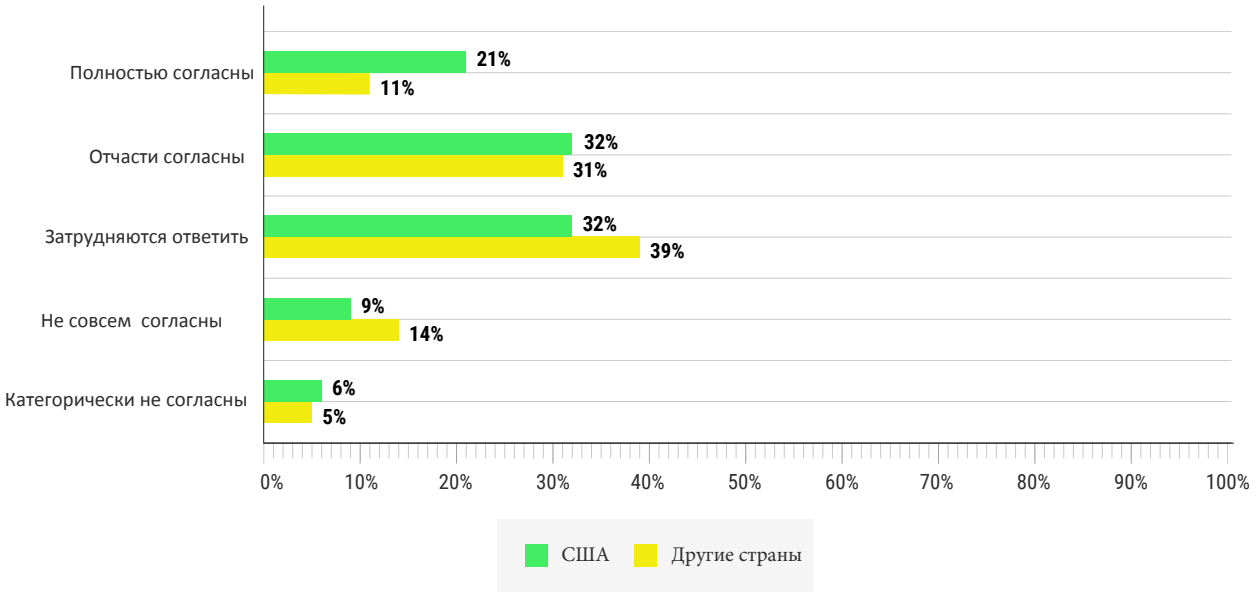
Вопрос: Насколько вы согласны с тем, что ваша организация готова к киберинциденту и знает, как на него реагировать?

Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

Ландшафт и проблемы кибербезопасности

Пандемия COVID-19 спровоцировала глобальный ажиотаж, позволивший работникам, компаниям и государственным учреждениям работать удаленно. Хотя бизнес и общество выиграют от этой цифровой трансформации, она усилила уязвимость во всем мире и во всех секторах промышленности. Нигде наши риски так не высоки, как среди малого и среднего бизнеса. Тем не менее, многие малые и средние предприятия не располагают финансовыми ресурсами или человеческим потенциалом для решения проблем кибербезопасности и не видят большой отдачи от инвестиций, тратя скудные ресурсы на кибербезопасность. Согласно исследованию CRI 2021 года, только 21% малых и средних предприятий уверены, что время и деньги, которые их организация вкладывает в кибербезопасность, снизят их риск. Большинство малых и средних предприятий чаще всего не уверены в ценности инвестиций в кибербезопасность. Между тем, многие крупные организации не имеют даже основных требований к кибербезопасности для своих поставщиков малого и среднего бизнеса или только начинают решать эту проблему.

Только 21% малых и средних предприятий США уверены в том («полностью согласны с тем»), что деньги, вложенные в кибербезопасность, снижают их риск.

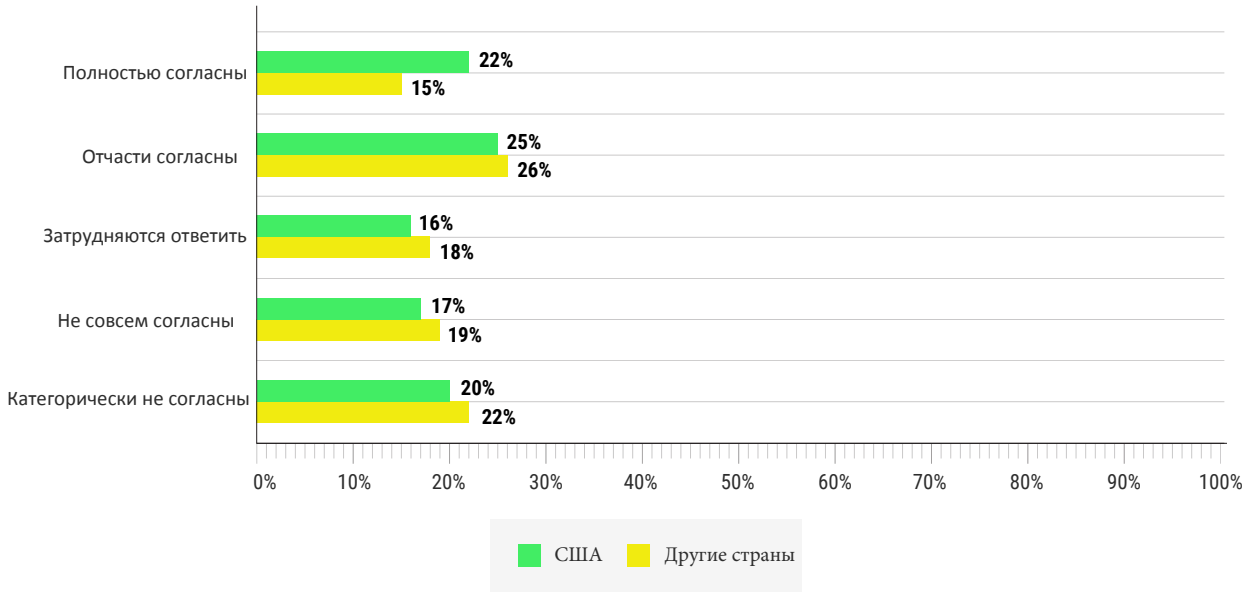


Вопрос: В какой степени вы согласны с тем, что время и деньги, которые ваша организация инвестирует в кибербезопасность, снижают ваш риск?

Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

Существует множество угроз для малого и среднего бизнеса, но программы-вымогатели, фишинг и кража учетных данных (кража паролей) являются одними из самых серьезных. Ожидается, что эти угрозы будут только расти, поскольку отрасли продолжают переводить все операции в онлайн среду из-за пандемии COVID-19 и меняющегося характера работы. Эти быстрые изменения привели к пробелам в киберустойчивости, поскольку фирмы, особенно с меньшими ресурсами, изо всех сил стараются не отставать. Эти увеличивающиеся уязвимости легко и часто используются злоумышленниками.

Только 22% малых и средних предприятий США уверены в том («полностью согласны с тем»), что у них есть сотрудник или группа сотрудников с четкой ответственностью за кибербезопасность.



Вопрос: В какой степени вы согласны со следующим утверждением: «У нас есть сотрудник или группа сотрудников, несущих четкую ответственность за нашу кибербезопасность»?

Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

Последствия компрометации кибербезопасности имеют отношение не только к рассматриваемой компании, но и к другим предприятиям в их цепочке поставок. Учитывая, что более двух третей крупных предприятий передают часть своих функций на аутсорсинг и разрешают третьим сторонам доступ к своим данным, недостаточная киберзащита среди малого и среднего бизнеса может иметь последствия и для более крупных фирм. **Отчет за 2020 год, составленный Accenture, показал, что до 40% кибервзломов являются косвенными, то есть они нацелены на слабые звенья в цепочках поставок или бизнес-экосистемах.**

Рекомендации

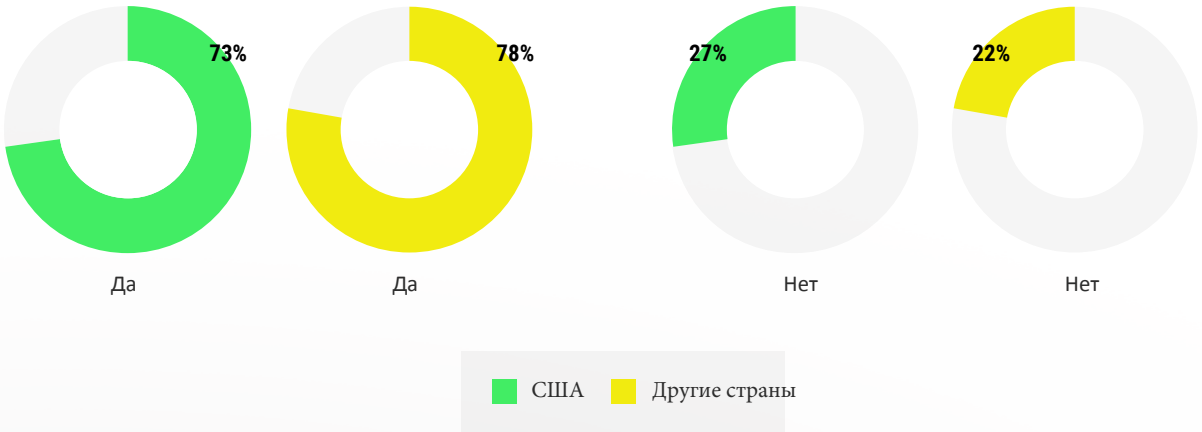
Кибербезопасность малого и среднего бизнеса США является неотъемлемой частью беспрепятственной работы наших государственных и частных учреждений и экономического благосостояния нашей страны. Ниже приведены пять рекомендаций, которые помогут подготовить малый и средний бизнес США к кибербезопасности.

- Создать национальную информационную кампанию для повышения киберготовности малого и среднего бизнеса
- Создать ресурсный центр по кибербезопасности для малого и среднего бизнеса в рамках федерального правительства
- Предложить налоговые льготы, чтобы побудить малый и средний бизнес инвестировать в кибербезопасность
- Установить государственно-частное сотрудничество для разработки минимальных стандартов кибербезопасности
- Создать финансируемые государством киберотряды в сотрудничестве с сообществом и 4-летними колледжами

Создание национальной информационной кампании для повышения киберготовности малого и среднего бизнеса

Как нация, у нас есть долгая история применения кампаний по информированию общественности для спасения жизней и изменения поведения — от кампаний для лесных пожаров до ремней безопасности и рекламы «Увидел что-то, скажи» после 11 сентября. Настало время для национальной кампании по повышению осведомленности, которая сосредоточена на роли человеческого поведения в области кибербезопасности и ознакомит всех с действиями, которые обеспечат всем нам безопасность. Общество поддерживает государственную кампанию: согласно опросу CRI 2021 года, более 60% малых и средних предприятий США и всего мира считают, что правительству следует создать национальную кампанию по повышению осведомленности общественности с целью усиления киберготовности.

Более 70% малых и средних предприятий США хотят, чтобы правительство предпринимало больше усилий по киберподготовке оорганизаций в цепочке поставок



Вопрос: Должно ли правительство предложить дополнительную поддержку, чтобы помочь вам улучшить кибербезопасность вашей организации и других участников цепочки поставок?

Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

info@cyberreadinessinstitute.org

Кибербезопасность — сложная область, которую нелегко свести к простому сообщению. Эффективная общественная кампания должна быть сосредоточена на одной основной проблеме кибербезопасности, например, на использовании надежных паролей. Освещение одной темы с помощью простого повторяющегося сообщения поможет защитить малый и средний бизнес от одного из методов, которым отдают предпочтение хакеры.

Создание ресурсного центра по кибербезопасности для малого и среднего бизнеса в рамках федерального правительства

Национальная информационная кампания, направленная на киберготовность, естественным образом направит малый и средний бизнес к списку доступных государственных и частных ресурсов. Сегодня эти ресурсы разбросаны по нескольким государственным учреждениям, иногда с советами, которые слишком сложны для многих владельцев бизнеса, у которых нет собственного ИТ-персонала или которые отдают кибербезопасность на аутсорсинг. Учитывая текущую работу Агентства по кибербезопасности и безопасности инфраструктуры (CISA) для малого и среднего бизнеса, мы рекомендуем, чтобы CISA было агентством, которое лучше всего подходит для курирования ресурсов кибербезопасности для МСП. Агентство, уполномоченное курировать ресурсы, также должно иметь своей основной задачей упрощение концепций, связанных с кибербезопасностью, чтобы сделать их понятными и доступными для владельцев бизнеса.

Предложение налоговых льгот с тем, чтобы побудить малый и средний бизнес инвестировать в кибербезопасность

Чтобы стимулировать инвестиции малого и среднего бизнеса в кибербезопасность, федеральное правительство должно предоставить стимул в виде налоговых льгот. Министерству финансов в сотрудничестве с Управлением по делам малого бизнеса (SBA) и CISA следует разработать руководящие принципы для инвестиций малого и среднего бизнеса в кибербезопасность, чтобы иметь право на получение налоговых льгот. В то время как налоговые льготы сократят сумму налогооблагаемого дохода, который собирает правительство, улучшение кибербезопасности снизит экономический ущерб, наносимый кибератаками, и окажет положительное влияние на безопасность, силу и устойчивость цифровой экономики.

Работая с другими агентствами и запрашивая мнение отрасли, Министерство финансов может установить требования к компаниям, чтобы указать, что они предприняли шаги для киберподготовки, прежде чем получать какие-либо налоговые льготы. Эти стандарты должны требовать обучения и образования сотрудников в области кибербезопасности, чтобы они могли претендовать на получение кредита. Образование должно подчеркивать необходимость создания культуры кибербезопасности на рабочем месте. Осведомленность о рисках, связанных с кибервзломами, и о поведении, которое снижает эти риски, должна отражаться в действия всех членов команды - от сотрудников до руководства, чтобы сотрудники понимали свои обязанности, и были предприняты действия для обеспечения готовности организации к кибератакам.

Установление государственно-частного сотрудничества с целью разработки минимальных стандартов кибербезопасности

Мы больше не можем полагаться на рыночные силы или добровольные действия для улучшения кибербезопасности наших государственных и частных учреждений. В настоящее время «первый выход на рынок» важнее «безопасного выхода на рынок». Рыночные силы отдают предпочтение прибыли, а не безопасности, и создают уязвимости, которые наши противники легко выявляют. Эта структура неприемлема и должна быть изменена. Мы должны создать стандарты, которые отдают приоритет безопасности на рынке. В сочетании с эффективной просветительской и информационной кампанией рыночные стандарты безопасности также помогут потребителям сделать безопасность приоритетной.

Установление стандартов в рамках сотрудничества между промышленностью и правительством имеет жизненно важное значение для обеспечения безопасности цепочек поставок. Мы успешно установили правила, которые повышают безопасность наших дорог, здравоохранения и финансовых систем. Точно также мы должны установить минимальные стандарты кибербезопасности.

Не существует универсального решения для подготовки организаций к кибератакам. Количество сотрудников, отрасль, технические знания и финансовые возможности — вот лишь несколько факторов, которые зависят от компании. Но промышленность и правительство могут работать вместе, чтобы установить стандарты, ориентированные на подход к управлению рисками, которые учитывают эти факторы.

Создание киберотрядов, финансируемых государством, в сотрудничестве с сообществом и 4-летними колледжами

Государственная программа, финансируемая за счет грантов, присуждаемых Национальным научным фондом, уже существует: CyberCorps: Scholarship for Service. Однако эта программа предназначена для набора и обучения ИТ-специалистов и менеджеров по кибербезопасности для работы в федеральных, государственных и местных агентствах. Новая программа Cyber Squad расширит поток талантов, доступных для малого и среднего бизнеса, а также будет способствовать привлечению различных дисциплин и опыта для создания культуры киберготовности в малых и средних предприятиях.

Cyber Squads могут решить несколько проблем, которые мешают малым и средним предприятиям стать киберготовыми включая нехватку кадров и финансовых ресурсов. Программа Cyber Squad, созданная по образцу Корпуса мира, или кампания, аналогичная образовательной инициативе по науке, технологиям, инженерии и математике (S.T.E.M.), позволит учащимся изучить интерес к кибербезопасности в качестве карьерного пути, обеспечивая при этом связь со своими местными сообществами.

В сотрудничестве с местными колледжами и университетами студенты-стажеры, обладающие опытом работы в различных дисциплинах, получат дополнительное обучение тому, какую роль играет человеческое поведение в обеспечении безопасности малых и средних предприятий — таким вопросам, как управление паролями, обновление программного обеспечения и предупреждение о фишинге, которые не учитываются во многих программах кибербезопасности. Киберотряды будут отправлены в сообщество, чтобы помочь местным малым и средним предприятиям повысить их уровень киберготовности. Первоначально программа была сосредоточена на оказании помощи малофинансируемым предприятиям, принадлежащим меньшинствам.

Вывод

Эти рекомендации и действия подчеркивают насущную необходимость сотрудничества государственного и частного секторов для устранения серьезных уязвимостей, которые ставят под угрозу нашу национальную безопасность и экономическое благополучие. **Сейчас, как никогда ранее, нам необходимо активное, целенаправленное сотрудничество и коллективные действия между правительством и промышленностью.**

Киберсобытия прошлого года демонстрируют то, как наши киберпреступники становятся все более изощренными в выявлении наших уязвимостей и слабостей и использовании их. Мы должны укреплять наши возможности киберзащиты, продолжая инвестировать в нашу готовность атаковать.

Малым и средним предприятиям необходим доступ к ресурсам кибербезопасности, которые носят предписывающий характер и доступны. Ресурсы, инструменты и методы для малого и среднего бизнеса требуют подхода, отличного от того, который нужен более крупным предприятиям. Цель та же — создать здоровую защищенную компанию, но путь к ней другой. Мы не можем просто сократить инструменты и методы, используемые крупными корпорациями, до меньших версий для малого и среднего бизнеса.

Мы должны проявлять инициативу в поддержке малых и средних предприятий, чтобы они стали сильной стороной нашей экосистемы, а не слабостью. Они должны стать более устойчивыми и киберготовыми, чтобы в нашей стране была прочная основа и культура безопасности.

Об Институте киберготовности

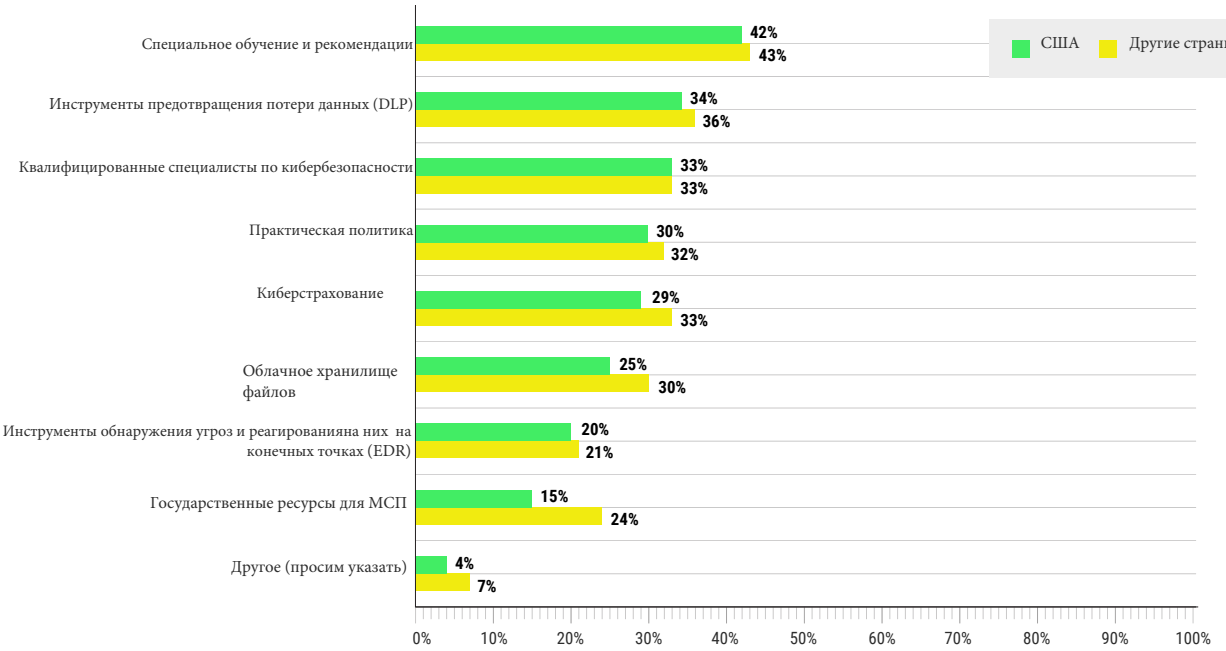
CYBER READINESS INSTITUTE

Институт кибербезопасности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые используются с целью разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). CRI был соучредителем руководителей The Center for Global Enterprise, Mastercard, Microsoft, PSP Partners в качестве продолжения работы Комиссии по повышению национальной кибербезопасности. Среди наших членов также ExxonMobil, General Motors и Principal. Наша миссия — повышать киберготовность малых и средних предприятий для укрепления безопасности глобальных цепочек поставок. Ресурсы CRI сосредоточены на человеческом поведении и делают упор на обучение и осведомленность сотрудников. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.

Приложение

Глобальное исследование кибербезопасности Института киберготовности*, январь 2021 г.

Большинству малых и средних предприятий требуется специальное обучение и рекомендации, чтобы сделать свою организацию более кибербезопасной.

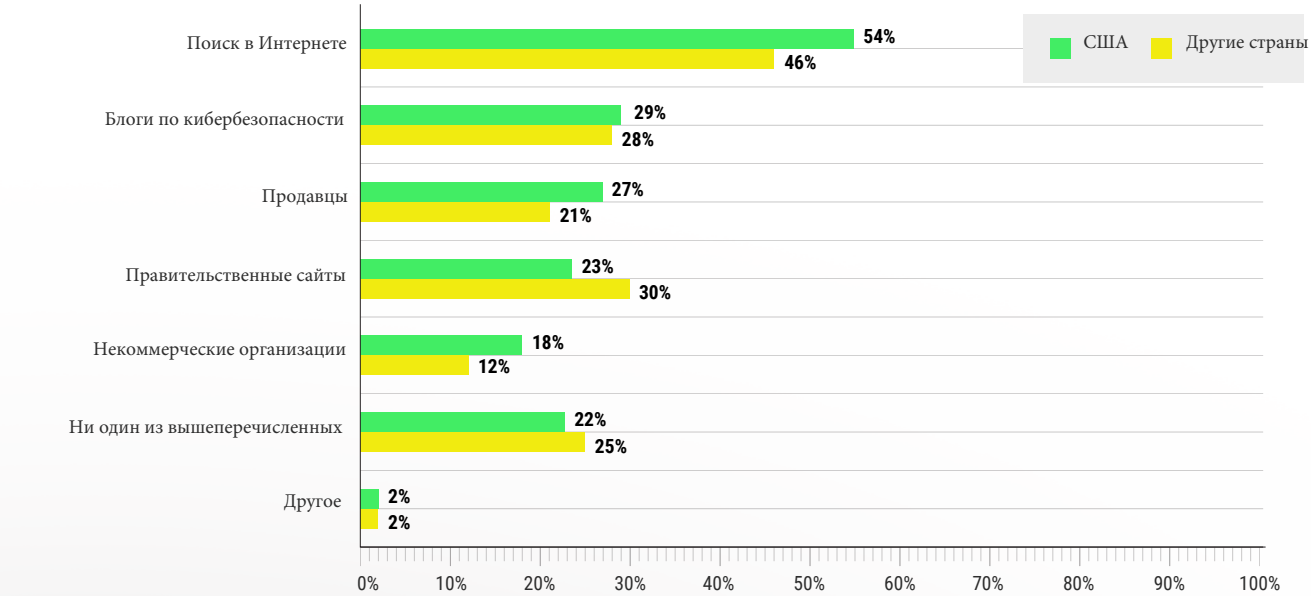


Вопрос. Что из перечисленного ниже необходимо для повышения безопасности вашей организации? (выберите все подходящие варианты)

Источник: Глобальный опрос Института киберготовности, исследование малого и среднего бизнеса, январь 2021 г.

**Масштаб опроса: США — 576 человек, весь мир – 517 человек.*

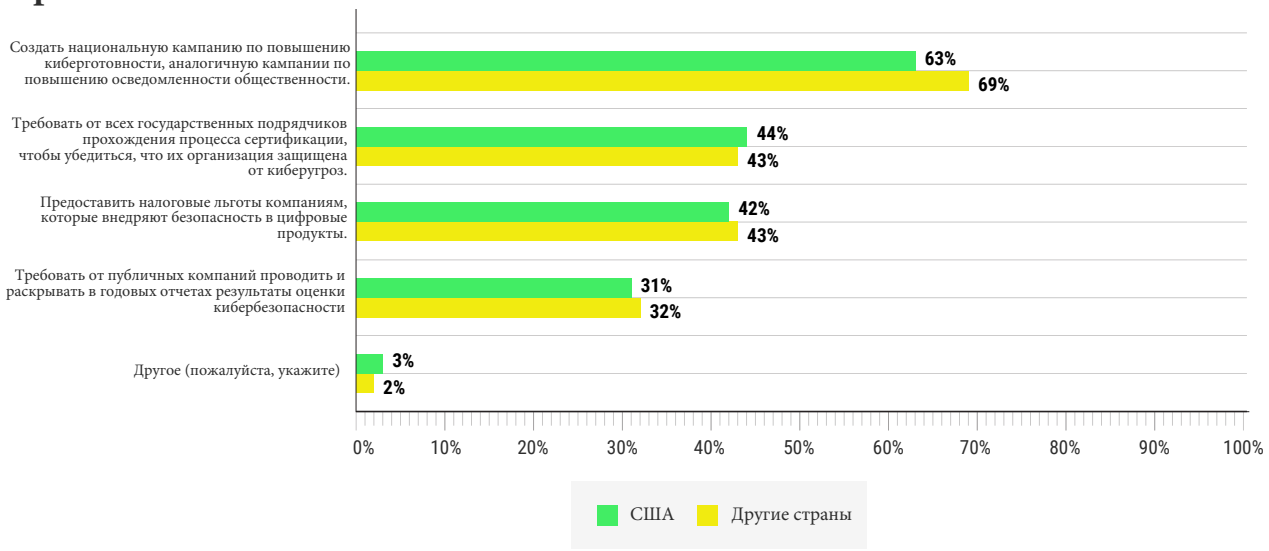
Большинство малых и средних предприятий полагаются на поиск ресурсов по кибербезопасности в Интернете.



Вопрос: К каким из следующих источников вы обращались, чтобы найти ресурсы по кибербезопасности для вашей организации? *Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.*

info@cyberreadinessinstitute.org

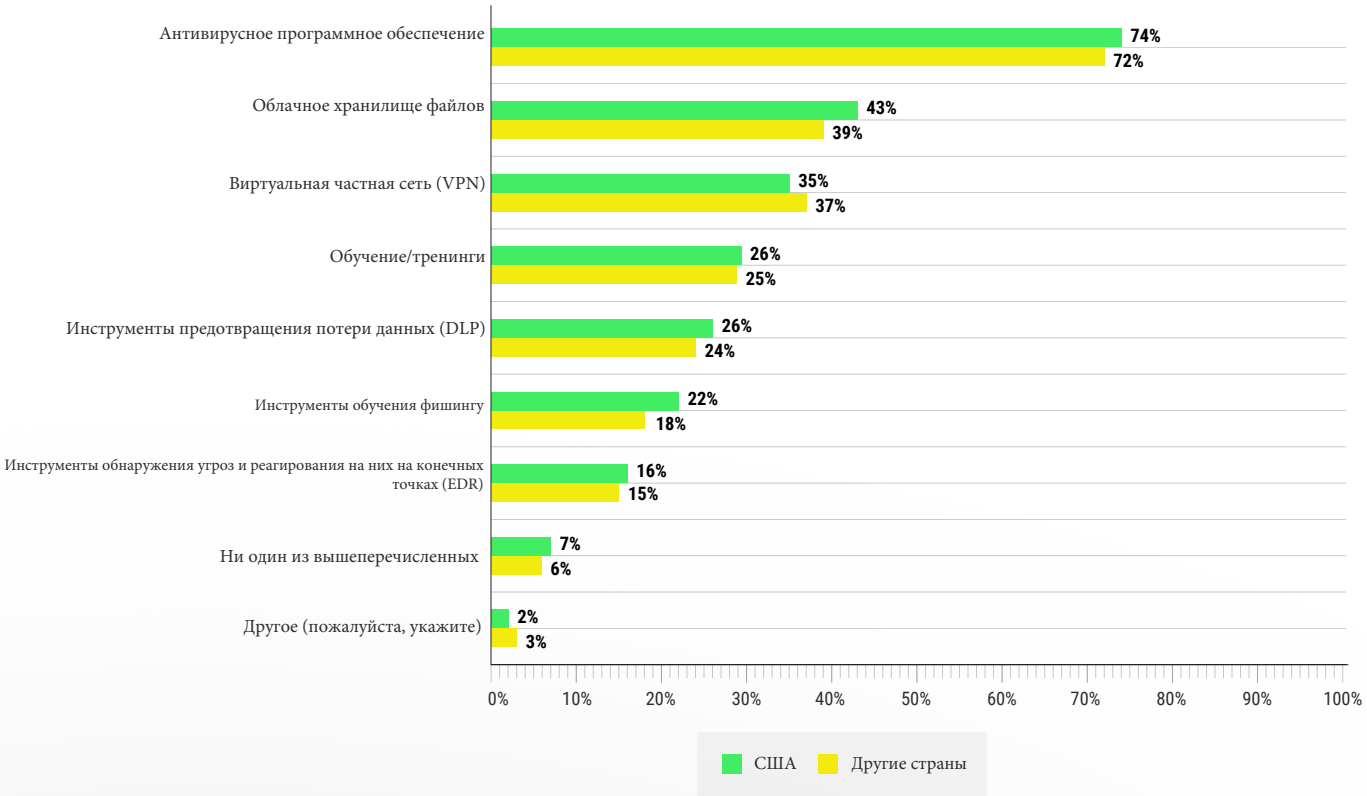
Более 60% малых и средних предприятий США хотят, чтобы правительство организовало национальную информационную кампанию для повышения киберготовности.



Вопрос: Какие из следующих шагов должно предпринять правительство?

Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

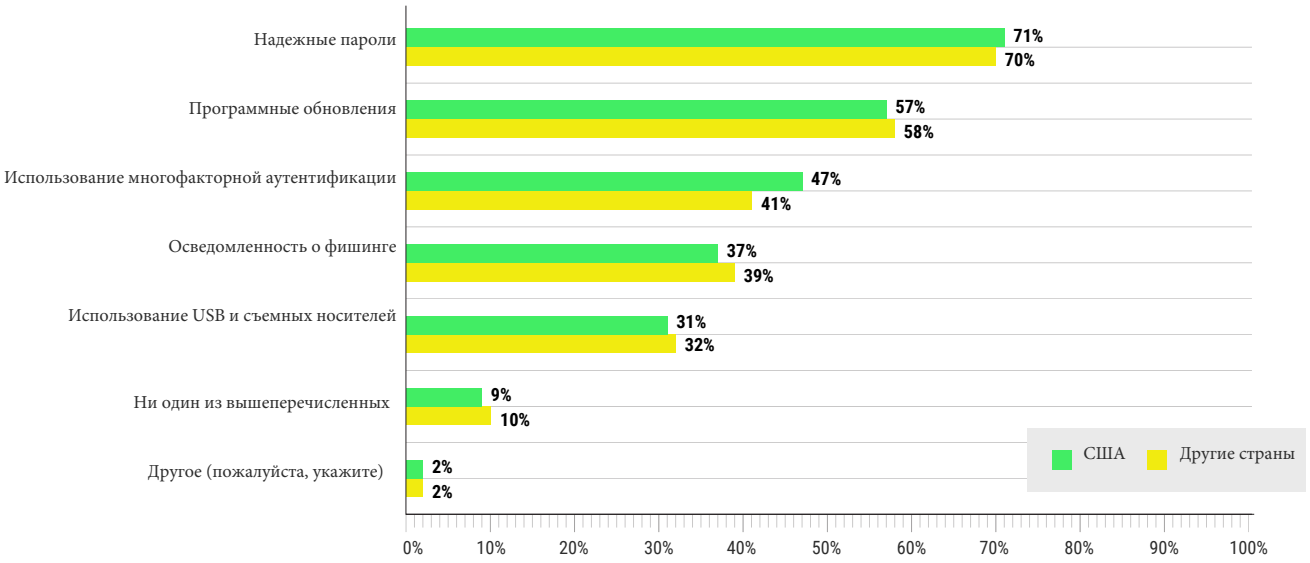
Антивирусное программное обеспечение, облачное хранилище файлов и виртуальная частная сеть (VPN) — это три основных инструмента кибербезопасности, на которые полагаются малые и средние предприятия.



Вопрос. Какие из следующих технологий и/или инструментов вы использовали для обеспечения кибербезопасности своей организации?

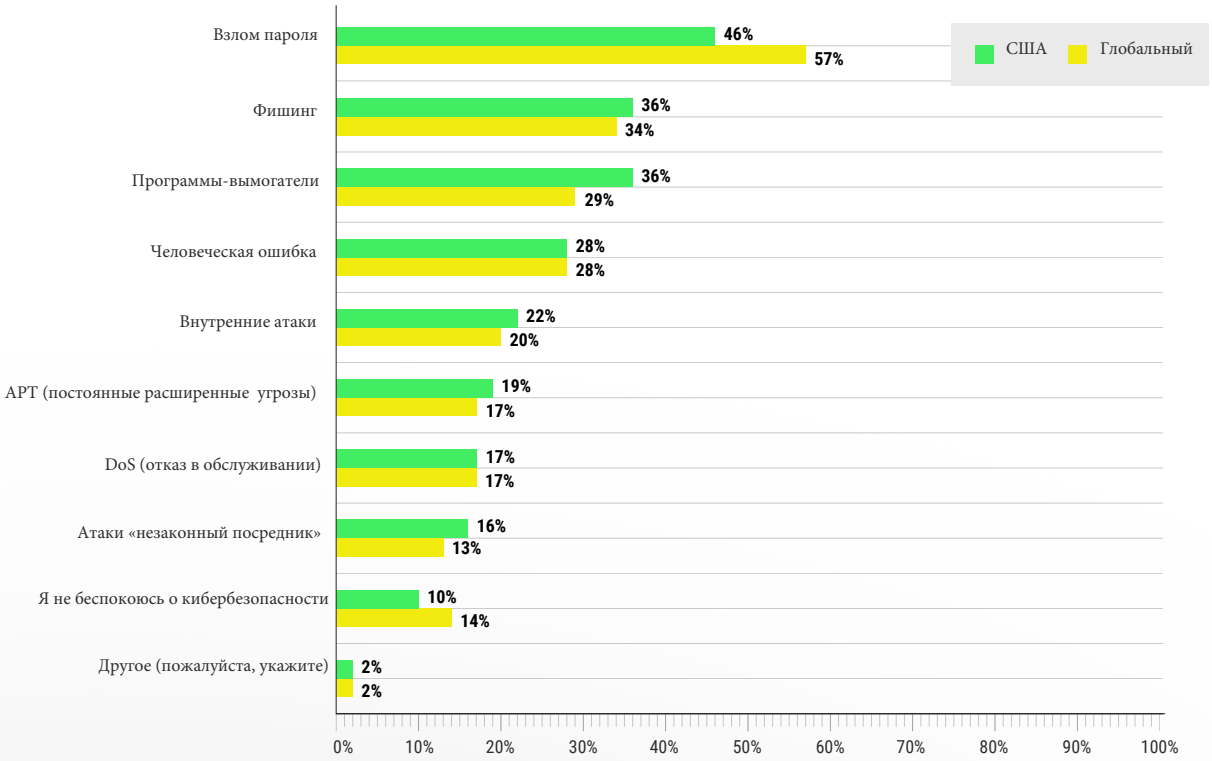
Источник: Глобальный опрос Института киберготовности, малый и средний бизнес, январь 2021 г.

71% малых и средних предприятий США говорят, что их сотрудники обучены использованию надежных паролей. НО слабые пароли по-прежнему являются основной причиной недавних взломов.



Вопрос. Каким из следующих тем, связанных с кибербезопасностью, обучены сотрудники вашей организации?
Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.

Взлом паролей возглавляет список проблем кибербезопасности среди малых и средних предприятий наряду с фишингом, программами-вымогателями и человеческими ошибками.



Вопрос: Что вас больше всего беспокоит в отношении кибербезопасности вашей организации?
Источник: Глобальный опрос Института киберготовности, Малый и средний бизнес, январь 2021 г.