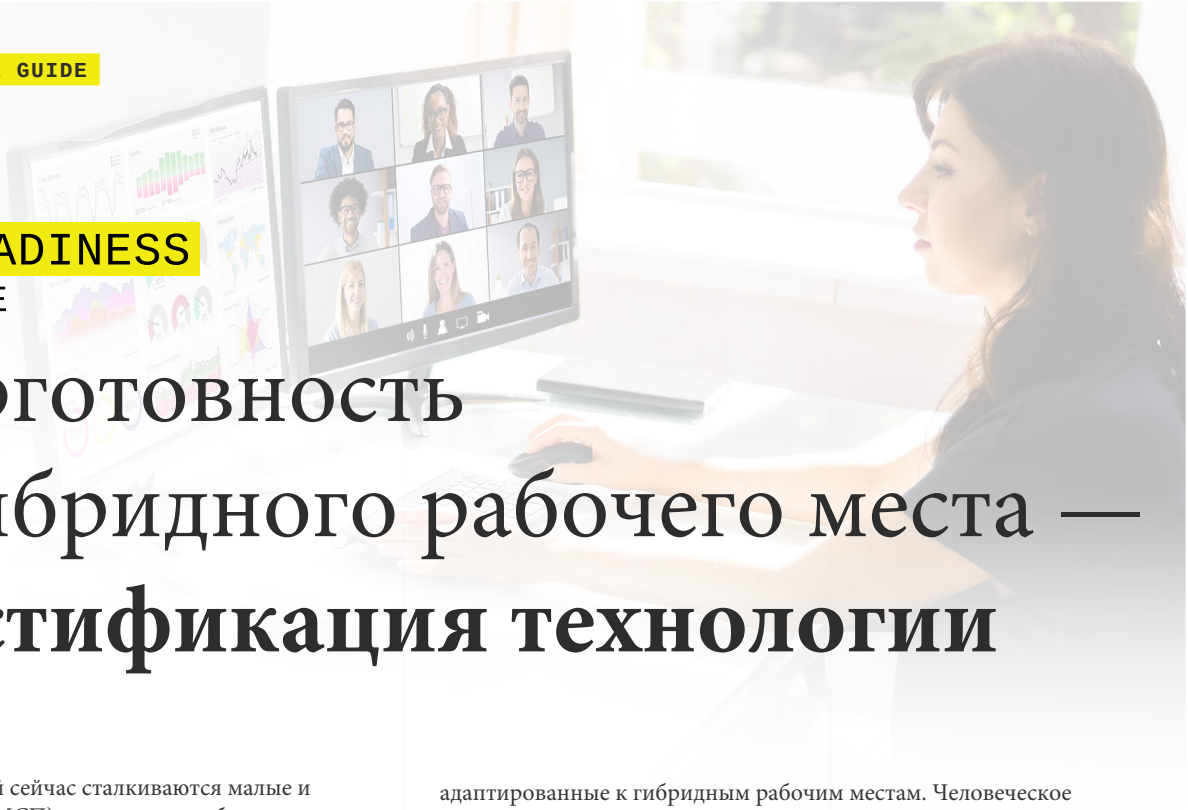


CYBER READINESS
INSTITUTE

Киберготовность для гибридного рабочего места — **демистификация технологии**

Вот ситуация, с которой сейчас сталкиваются малые и средние предприятия (МСП): сотрудники работают из дома, офиса и других мест (даже на открытом воздухе, если позволяет погода). Они используют корпоративные и персональные устройства. Сотрудники получают доступ к документам или передают их из одного места в другое и с одного устройства на другое. Они обмениваются документами с другими сотрудниками и третьими лицами. Хакеры систематически сканируют сети, стремясь воспользоваться новыми уязвимостями.

Гибридное рабочее место создает новые большие проблемы кибербезопасности для организаций всех масштабов. Людям необходимо выработать новые привычки, а организациям - внедрить новые политики, адаптированные к гибридным рабочим местам. Человеческое поведение является основой безопасности во всех организациях.

Однако организациям также необходимо рассмотреть возможность развертывания новой технологии для гибридных рабочих мест. Когда сотрудники перемещаются из одного места в другое, они могут использовать различные устройства. Они определенно используют различные виды соединения для доступа к вашей сети и данным из разных мест. Доступ на гибридном рабочем месте создает уязвимости и возможность для путаницы и хаоса.

Малым и средним предприятиям мы рекомендуем рассматривать гибридное рабочее место с точки зрения устройств, подключений и данных. Вот основные вопросы, на которые вам нужно ответить:

Устройства:

1. **Какие устройства используют сотрудники?**
2. **Используют ли они одни и те же устройства независимо от того, где находятся?**

Связь:

1. **Как удаленные сотрудники подключаются к вашей сети?**
2. **Как сотрудники подключаются к вашей сети в офисе компании?**

Данные

1. **Как сотрудники получают доступ к данным с каждого устройства и места?**
2. **К каким данным они имеют доступ?**
3. **Как сотрудники передают данные с устройства на устройство, из одного места в другое, а также другим сотрудникам или третьим лицам?**
4. **Как и где сотрудники хранят данные?**

guide@cyberreadinessinstitute.com

Существуют различные технологии, позволяющие снизить риск кибербезопасности, включая огромное количество вариантов аппаратного и программного обеспечения. Задача малых и средних предприятий состоит в том, чтобы понять, инвестиции в какие технологии могут значительно снизить риск кибербезопасности, а какие технологии обеспечат безопасное поведение сотрудников, а не поощрение обходных путей.

Рассматривать технологии с точки зрения устройств, подключений и данных — это эффективный способ оценить свои возможности и принять решение. При выборе технологии количество сотрудников и ваш бюджет, конечно же, будут иметь огромное влияние на то, что можно предпринять. Вот несколько соображений, с которых мы советуем начать.

Устройства:

1. **Компьютеры и/или планшеты, выданные компанией**, снизят ваш риск и предоставят вам больший контроль над тем, какое программное обеспечение установлено, обновлениями программного обеспечения, сканированием на наличие вирусов и вредоносных программ и т. д. — если вы можете себе это позволить. В качестве альтернативы можно рассмотреть инфраструктуру виртуальных рабочих столов (см. ниже).

2. **Смартфоны, выданные компанией.** В зависимости от вашего бизнеса и того, как люди работают, подумайте также о выдаче компанией смартфонов. Люди большую часть своего личного времени проводят, используя смартфон, а уязвимости, создаваемые социальными и развлекательными приложениями, могут обеспечить доступ к сети вашей компании, если она не защищена должным образом. Смартфоны, выданные компанией, могут вызывать разногласия, так как людям не нравится носить с собой два телефона. Как менеджер вы должны принимать обоснованные решения по управлению рисками.

Соединения:

1. **Виртуальная частная сеть (VPN).** VPN — важная базовая защита, когда люди работают удаленно. Она создает частный, безопасный канал между домом сотрудника и вашей сетью.

2. **Сегрегация домашней сети сотрудника**. Если сотрудники получают доступ к ценной и конфиденциальной информации, помогите им настроить собственную домашнюю сеть Wi-Fi с отдельным паролем.

3. **Точка доступа, предоставляемая компанией.** Некоторые современные мобильные точки доступа имеют встроенный VPN. Эти точки доступа могут быть хорошей альтернативой использованию общей Wi-Fi сети или своего личного телефона в качестве точки доступа. Кроме того, точка доступа, предоставленная компанией, является хорошим вариантом для сотрудников, которые работают из нескольких удаленных мест.

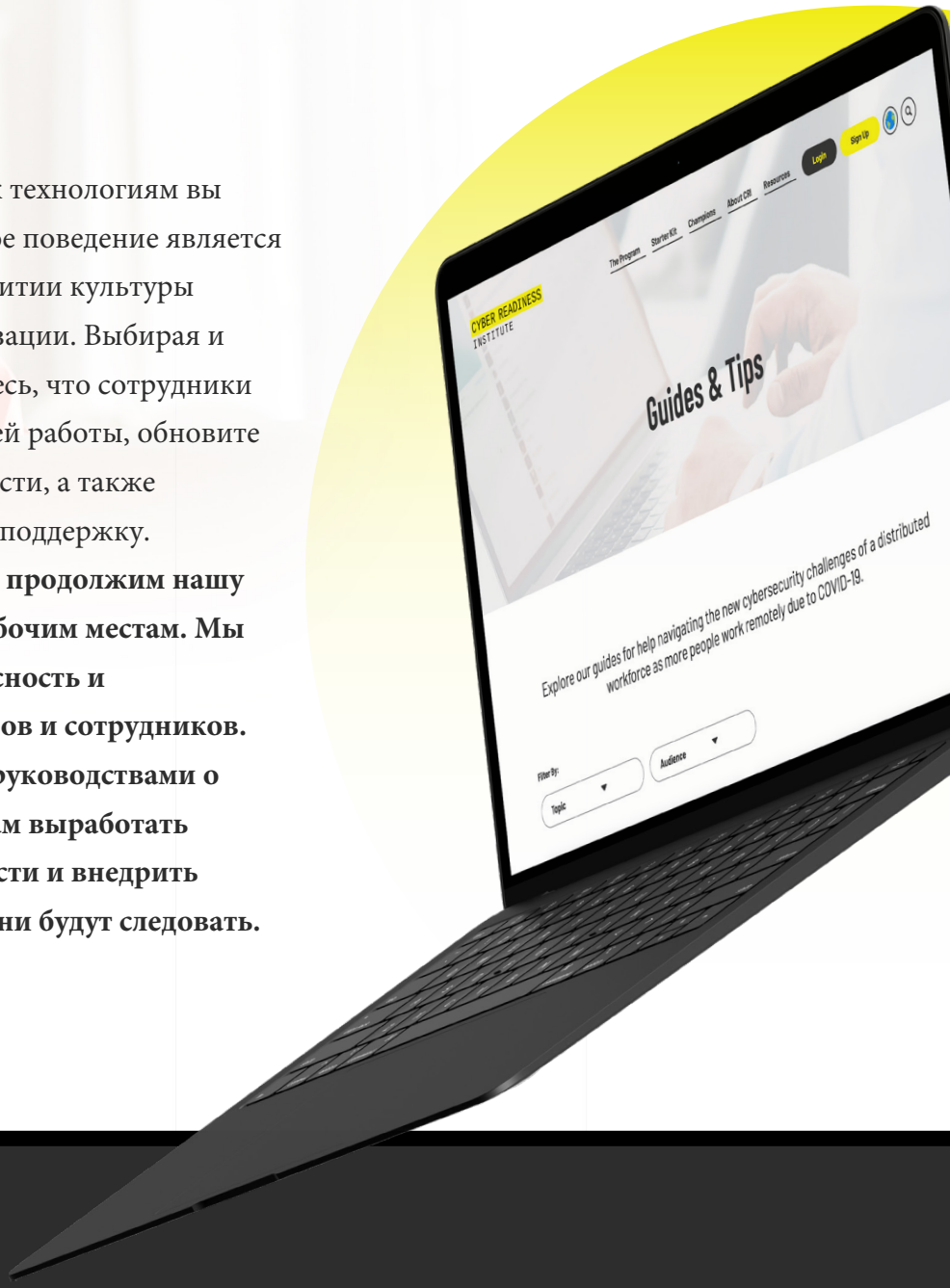
Данные:

1. **Облачный обмен файлами.** Отличный вариант для начала. Этот общий доступ к файлам устраняет многие проблемы безопасности с доступом к данным, их передачей и хранением, когда сотрудники работают из нескольких мест, поскольку все документы хранятся централизованно. Однако это требует от людей изменения своего поведения и выработки новых привычек таких, как: а) организованный подход к местоположению документов; и б) процесс контроля версий. Компании также должны убедиться, что сотрудники имеют надежные и безопасные соединения (см. выше), когда они работают удаленно с тем, чтобы обеспечить безопасность системы обмена файлами.

2. **Инфраструктура виртуальных рабочих столов (VDI):** VDI означает, что «рабочий стол» сотрудников находится не на их устройстве. Он находится на сервере, к которому они могут получить доступ с любого устройства, и можно отказаться от необходимости в предоставлении устройств, выдаваемых компанией. Приложения и данные существуют только на сервере, поэтому ими можно управлять централизованно. Это предложение часто поставляется в комплекте с облачными сервисами, программным обеспечением и ПО для кибербезопасности.

Независимо от того, какой подход к технологиям вы выберете, помните, что человеческое поведение является наиболее важным элементом в развитии культуры кибербезопасности в вашей организации. Выбирая и внедряя новую технологию, убедитесь, что сотрудники могут ее использовать с учетом своей работы, обновите свои политики по мере необходимости, а также обеспечьте обучение и постоянную поддержку.

Оставайтесь с нами, поскольку мы продолжим нашу серию обучения по гибридным рабочим местам. Мы объясним, что такое кибербезопасность и предоставим советы для менеджеров и сотрудников. Ознакомьтесь с другими нашими руководствами о том, как помочь своим сотрудникам выработать хорошие привычки киберготовности и внедрить практические правила, которым они будут следовать.

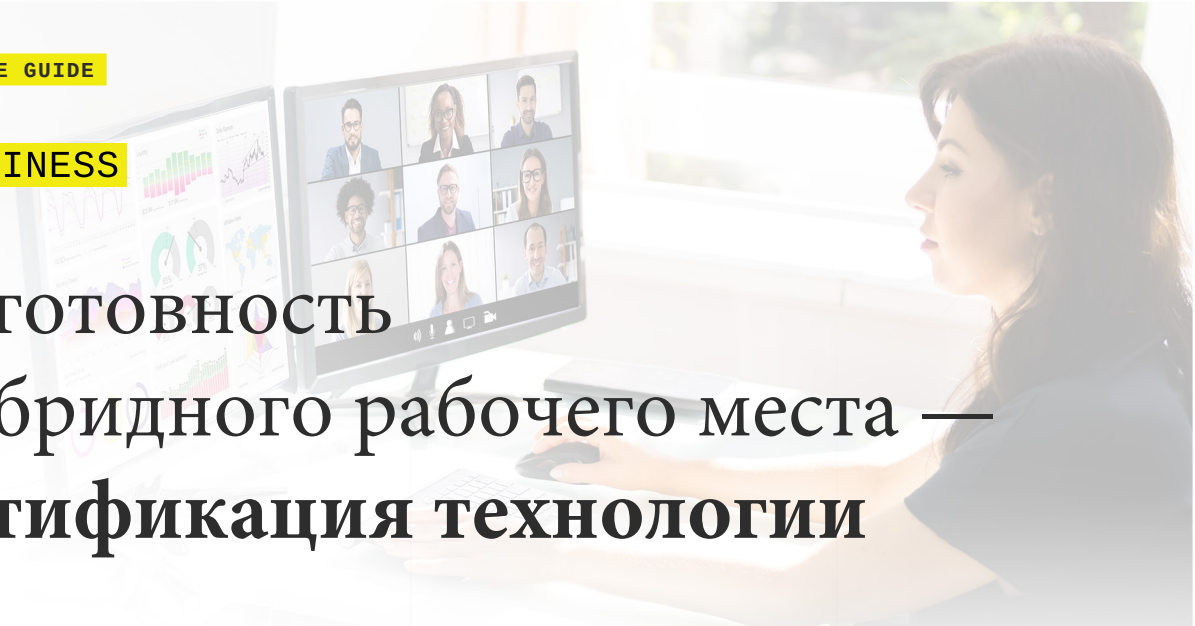


CYBER READINESS
INSTITUTE

Об Институте киберготовности

Институт киберготовности — 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). Изучите основы хорошей кибербезопасности с помощью нашего Стартового набора или создайте культуру кибербезопасности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.

CYBER READINESS
INSTITUTE



Киберготовность для гибридного рабочего места — **демистификация технологии**

Вот ситуация, с которой сейчас сталкиваются малые и средние предприятия (МСП): сотрудники работают дома, в офисе и в других местах (даже на открытом воздухе, если позволяет погода). Они используют корпоративные и персональные устройства. Сотрудники получают доступ к документам или передают их из одного места в другое и с одного устройства на другое. Они обмениваются документами с другими сотрудниками и третьими лицами. Хакеры систематически сканируют сети, стремясь воспользоваться новыми уязвимостями.

Гибридное рабочее место создает большие проблемы кибербезопасности для организаций всех масштабов. Людям необходимо выработать новые привычки, а организациям - внедрить политику, адаптированную к гибридному рабочему месту. Человеческое поведение является основой безопасности во всех организациях.

Однако организациям также необходимо рассмотреть возможность развертывания новой технологии для гибридных рабочих мест. Когда сотрудники перемещаются из одного места в другое, они могут использовать различные устройства. Они определенно используют различные соединения для доступа к вашей сети и данным из разных мест. Доступ на гибридном рабочем месте создает уязвимости и возможность для путаницы и хаоса.

Малым и средним предприятиям мы рекомендуем рассматривать гибридное рабочее место с точки зрения устройств, подключений и данных. Вот основные вопросы, на которые вам нужно ответить:

Устройства:

1. **Какие устройства используют сотрудники?**
2. **Используют ли они одни и те же устройства независимо от того, где находятся?**

Связь:

1. **Как удаленные сотрудники подключаются к вашей сети?**
2. **Как сотрудники подключаются к вашей сети в офисе компании?**

Данные:

3. **Как сотрудники получают доступ к данным с каждого устройства и места?**
4. **К каким данным они имеют доступ?**
5. **Как сотрудники передают данные с устройства на устройство, из одного места в другое, а также другим сотрудникам или третьим лицам?**
6. **Как и где люди хранят данные?**

Существуют различные технологии, позволяющие снизить риск кибербезопасности, включая огромное количество вариантов аппаратного и программного обеспечения. Задача малых и средних предприятий состоит в том, чтобы понять, какие инвестиции в технологии могут значительно снизить риски кибербезопасности, а какие технологии обеспечат безопасное поведение сотрудников, а не поощрение обходных путей.

Рассматривать технологии с точки зрения устройств, подключений и данных — это эффективный способ оценить свои возможности и принять решение. При выборе технологии количество сотрудников и ваш бюджет, конечно же, будут иметь огромное влияние на то, что можно предпринять. Вот несколько соображений, с которых мы советуем начать.

guide@cyberreadinessinstitute.com

Устройства:

1.**Компьютеры и/или планшеты, выданные компанией**, снизят ваш риск и предоставят вам больший контроль над тем, какое программное обеспечение установлено, обновлениями программного обеспечения, сканированием на наличие вирусов и вредоносных программ и т. д. — если вы можете себе это позволить. В качестве альтернативы можно рассмотреть инфраструктуру виртуальных рабочих столов (см. ниже).

2. **Смартфоны, выданные компанией.** В зависимости от вашего бизнеса и того, как люди работают, подумайте также о выдаче компанией смартфонов. Люди большую часть своего личного времени проводят, используя смартфон, а уязвимости, создаваемые социальными и развлекательными приложениями, могут обеспечить доступ к сети вашей компании, если она не защищена должным образом. Смартфоны, выданные компанией, могут вызывать разногласия, так как людям не нравится носить с собой два телефона. Как менеджер вы должны принимать обоснованные решения по управлению рисками.

Соединения:

1. **Виртуальная частная сеть (VPN).** VPN — важная базовая защита, когда люди работают удаленно. Она создает частный, безопасный канал между домом сотрудника и вашей сетью.

2. **Сегрегация домашней сети сотрудника**. Если сотрудники получают доступ к ценной и конфиденциальной информации, помогите им настроить собственную домашнюю сеть Wi-Fi с отдельным паролем.

3. **Точка доступа, предоставляемая компанией.** Некоторые современные мобильные точки доступа имеют встроенный VPN. Эти точки доступа могут быть хорошей альтернативой использованию общей Wi-Fi сети или своего личного телефона в качестве точки доступа. Кроме того, точка доступа, предоставленная компанией, является хорошим вариантом для сотрудников, которые работают из нескольких удаленных мест.

Данные:

1. **Облачный обмен файлами.** Отличный вариант для начала. Этот общий доступ к файлам устраняет многие проблемы безопасности с доступом к данным, их передачей и хранением, когда сотрудники работают из нескольких мест, поскольку все документы хранятся централизованно. Однако это требует от людей изменения своего поведения и выработки новых привычек таких, как: а) организованный подход к местоположению документов; и б) процесс контроля версий. Компании также должны убедиться, что сотрудники имеют надежные и безопасные соединения (см. выше), когда они работают удаленно с тем, чтобы обеспечить безопасность системы обмена файлами.

2. **Инфраструктура виртуальных рабочих столов (VDI):** VDI означает, что «рабочий стол» сотрудников находится не на их устройстве. Он находится на сервере, к которому они могут получить доступ с любого устройства, и можно отказаться от необходимости в предоставлении устройств, выдаваемых компанией. Приложения и данные существуют только на сервере, поэтому ими можно управлять централизованно. Это предложение часто поставляется в комплекте с облачными сервисами, программным обеспечением и ПО для кибербезопасности.

Независимо от того, какой подход к технологиям вы выберете, помните, что человеческое поведение является наиболее важным элементом в развитии культуры кибербезопасности в вашей организации. Выбирая и внедряя новую технологию, убедитесь, что сотрудники могут ее использовать с учетом своей работы, обновите свои политики по мере необходимости, а также обеспечьте обучение и постоянную поддержку.

Оставайтесь с нами, поскольку мы продолжим нашу серию обучения по гибридным рабочим местам. Мы объясним, что такое кибербезопасность и предоставим советы для менеджеров и сотрудников. Ознакомьтесь с другими нашими руководствами о том, как помочь своим сотрудникам выработать хорошие привычки киберготовности и внедрить практические правила, которым они будут следовать.

Об Институте киберготовности

Институт киберготовности — 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). Изучите основы хорошей кибербезопасности с помощью нашего Стартового набора или создайте культуру кибербезопасности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.