УДК 002.304

НЕОБХОДИМОСТЬ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ УДАЛЁННОЙ РАБОТЕ И УДАЛЁННОМ ОБУЧЕНИИ

Дударева В. Н., студент
3 курс, факультет «38.04.02 Менеджмент (Управление в строительстве)»
Институт безотрывных форм обучения, Санкт-Петербургский государственный архитектурно-строительный университет
г. Санкт-Петербург, Россия

Аннотация

Статья посвящена методам и средствам необходимым для обеспечения информационной безопасности личных данных при удалённой работе и удалённом обучении. В настоящей статье рассматриваются особенности организации дистанционного соединения в России, его уязвимые места, как для частного использования, так и для корпоративного.

Ключевые слова

Удалённый формат работы, дистанционное обучение, корпоративная сеть, гибкий график, заражение компьютера, личные данные, безлопастное соединение.

student Dudareva V. N.
3rd year, faculty "38.04.02 Management (Management in construction)"
Institute of Continuous Forms of Education, St. Petersburg State University of Architecture and Civil Engineering
St. Petersburg, Russia

The need to use information security tools for remote work and remote learning

Annotation

The article is devoted to the method and means of protection for detecting confidential information during remote work and remote learning. The article discusses the features of remote connections in Russia, its vulnerability of the place, both for private use and for corporate use.

Keywords

Remote work format, distance learning, corporate network, flexible hours, computer shutdown, personal data, wireless connection.

Общество непрерывно изменяется, развиваются технологии, меняются подходы к реализации различных процессов. Необходимость изменений обуславливается различными факторами, такими как:

- текущая обстановка в регионе, стране, мире;
- увеличивающиеся потребности человечества;
- природными изменениями;
- открытиями в области науки;
- войнами.

Данные факторы требуют наличие изменений в различных отраслях, тем самым, вынуждая меняться и самих людей. Процесс изменения человека при воздействии на него тех или иных факторов можно назвать адаптацией, таким образом, для развития и существования общества способностью к адаптации должен владеть не только человек, но и отрасли деятельности.

В 2020 году общество столкнулось с проблемой распространения короновируса и было вынуждено принять ряд решений, который требует от человека и различных отраслей адаптации к этим решениям. Так, например, удалённая работа и дистанционное обучение используется во многих странах

мира, однако, такого масштаба использования как сейчас, ранее не наблюдалось. Связано это с тем, что в связи с угрозой заражения органы власти рекомендовали перевести сотрудников на удалённую работу, а школы и иные учебные заведения на дистанционное обучение. Тем самым, органы власти хотят снизить скорость распространения вируса для успешного оказания медицинской помощи всему населению, но не в момент времени, а на протяжении определённого периода. Тем самым, обеспечив медицинские структуры необходимым временным промежутком.

Разумеется, после таких рекомендаций и принятия соответствующих решений на уровне государственной власти в обществе начинается процесс адаптации к реализации новых технологий. К сожалению, не во всех сферах возможно удалённо работать, однако, смело можно заявить, что до 40% от общего числа работающих людей возможно или полностью, или частично перевести на удалённую работу. Такая процедура потребует некоторого времени, наличия ресурсов и адаптации сотрудников.

Дистанционное обучение осуществлять легче, по причине того, что молодое поколение способно быстрее адаптироваться к новым технологиям и подхода к обучению. Однако, присутствие проблем всё равно не избежать.

Помимо очевидных проблем и недостатков, которые в себе несёт дистанционное обучение и удалённая работа, существуют и другие, которые для менее очевидны, однако, несут в себе гораздо больше угроз, а именно угроз информационной безопасности.

При выполнении своих обязанностей сотрудник обычно использует рабочий компьютер, который подключён к корпоративной локальной сети. Как-правило, организации и предприятия обеспечивают тот или иной уровень защищённости корпоративной сети, а также самого компьютера сотрудника. Также, в средних и крупных компаниях существует отдел информационных технологий, либо отдел безопасности, функции которого предотвращение не только внешних атак и инцидентов, но и внутренних, например, угроз разглашения коммерческой тайны или распространения персональных

данных. Помимо этого, недобросовестные сотрудники при удалённой работе могут не качество или не в полной мере выполнять свои обязанности, тем самым принося ущерб компании.

При дистанционном обучении угроз информационной безопасности меньше, однако, они также существуют, поэтому нельзя недооценивать их.

Рассмотрим основные подходы к переводу сотрудников предприятия на удалённую работу:

- осуществление рабочей деятельности с собственного компьютера, без подключения к общей корпоративной сети;
- осуществление рабочей деятельности с собственного компьютера, с подключением к общей корпоративной сети тем или иным способом;
- осуществление рабочей деятельности с рабочего компьютера, находящегося дома у сотрудника без подключения к корпоративной сети;
- осуществление рабочей деятельности с рабочего компьютера, который находится дома у сотрудника с подключением к общей корпоративной сети и локальным сервисам.

Первый способ является самым простым для работодателя, так как задействуется минимум усилий со стороны работодателя для перевода сотрудников на удалённую работу, однако, он имеет множество отрицательных сторон:

- не у каждого сотрудника имеется дома персональный компьютер с выходом в интернет;
- многих сотрудников нельзя перевести на удалённую работу, т.к. специфика их деятельности требует либо личного присутствия, либо возможности подключения к локальной сети или локальным сервисам предприятия;
- некоторую часть обязанностей сотрудник не сможет выполнять по причине отсутствия специального программного обеспечения;

- отсутствие возможности контроля деятельности со стороны работодателя;
- риски распространения конфиденциальной информации;
- риски невыполнения требований законодательства в области информационной безопасности.

Второй способ более сложный в осуществлении, так как требует подключения к корпоративной сети и корпоративным сервисам предприятия, однако также имеет недостатки:

- не у каждого сотрудника имеется дома персональный компьютер с выходом в интернет;
- многих сотрудников нельзя перевести на удалённую работу, т.к. специфика их деятельности требует либо личного присутствия.
- угрозы информационных инцидентов из-за несоблюдения правил и инструкций по удалённой работе;
- угрозы заражения рабочего компьютера и корпоративной сети из-за обмена файлами между домашним и рабочим ПК.

Третий способ осуществляется легче, однако, также присутствуют риски, только другие:

- риски замены или похищения комплектующих рабочего компьютера;
- заражение рабочего компьютера;
- многих сотрудников нельзя перевести на удалённую работу, т.к. специфика их деятельности требует либо личного присутствия, либо возможности подключения к локальной сети или локальным сервисам предприятия;
- некоторую часть обязанностей сотрудник не сможет выполнять по причине отсутствия специального программного обеспечения;
- отсутствие возможности контроля деятельности со стороны работодателя;

- риски распространения конфиденциальной информации;
- риски невыполнения требований законодательства в области информационной безопасности.

Четвёртый способ перекрывает многие риски, однако, его осуществление осложнено и также несёт в себе угрозы:

- многих сотрудников нельзя перевести на удалённую работу, т.к. специфика их деятельности требует либо личного присутствия.
- угрозы информационных инцидентов из-за несоблюдения правил и инструкций по удалённой работе;
- риски замены или похищения комплектующих рабочего компьютера;
- заражение рабочего компьютера;
- риски распространения конфиденциальной информации;
- риски невыполнения требований законодательства в области информационной безопасности.

Таким образом, рассмотрев недостатки различных способов организации удалённого рабочего места, отметим, что дистанционное обучение подвержено в основном угрозам заражения своих компьютеров из-за несоблюдения правил информационной безопасности.

Отметим следующие рекомендации для обеспечения информационной безопасности на предприятии:

Рекомендуется использовать второй способ организации рабочего места.

Рабочий компьютер должен быть оснащён всем необходимым перечнем программного и аппаратного обеспечения: Антивирус желательно от Kaspersky; Secret Net Studio; ViPNet Client for Windows; МЭ.

Домашний компьютер должен быть оснащён хотя бы антивирусом.

Подключение к рабочему компьютеру рекомендуется осуществлять только по защищённым каналам.

Должны быть настроенные Политики безопасности на рабочих ПК сотрудников.

Должны быть подготовлены Инструкции для сотрудников, и администраторов информационной безопасности.

Сотрудникам, отвечающим за обеспечение информационной безопасности необходимо осуществлять мониторинг деятельности и предотвращение возможных инцидентов.

Необходимо исключить все возможные угрозы и риски.

С помощью выполнения данных рекомендаций невозможно полностью избавиться от рисков и угроз, однако, возможно их минимизировать. Следует учитывать, что основную роль в обеспечении защищённости информации при удалённой работе будут играть именно сотрудники, которые либо будут соблюдать инструкции и правила, либо нет. Второстепенную роль же занимают подразделения, обеспечивающие поддержку информационной инфраструктуры.

Касаемо дистанционного обучения, стоит отметить следующие рекомендации:

- ВУЗы должны использовать только проверенные платформы дистанционного обучения;
- нельзя допускать передачу конфиденциальной информации по незащищённом каналам;
- для учеников, учителей и преподавателей необходимо провести инструктаж по процедуре дистанционного обучения;
- необходимо составить Инструкции по дистанционному обучению, которые должны строго соблюдаться.

Используя все вышеприведенные рекомендации, возможно будет избежать многих угроз и инцидентов. Минимизируя минусы удалённой работы, возможно будет сконцентрироваться только на достоинствах и тем самым обеспечить более быструю адаптацию.

Использованные источники:

1. Ерохин, В.В. Безопасность информационных систем: учебное пособие / В.В. Ерохин. – М.: ФЛИНТА, 2015. – 182 с. – ISBN 978-5-9765-1904-6.

2. Малюк, А.А. Основы защиты информации: учебное пособие / А.А. Малюк. – М.: МИФИ, 2014. – 306 с. – ISBN 5-9916-2817-4.

3. Партыка, Т.Л. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. – М.: Форум, НИЦ ИНФРА-М, 2016. – 432 с. – ISBN 978-5-91134-627-0.

Информация об авторе:

Дударева Валерия Николаевна, студент 3 курс, факультет «38.04.02 Менеджмент (Управление в строительстве)» Институт безотрывных форм обучения, Санкт-Петербургский государственный архитектурно-строительный университет, Россия, г. Санкт-Петербург, + 7 926-96-26-357, valeriadydareva@gmail.com