УДК 004.056

Е.С. Асс [1]***, А.А. Бутин*** [1]

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

МЕТОДИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДИСТАНЦИОННОМ РЕЖИМЕ РАБОТЫ ОРГАНИЗАЦИИ

Аннотация. Рассмотрены преимущества и недостатки удаленной работы, как для самих сотрудников, так и для работодателей. Определены основные риски утечки корпоративных данных в режиме удаленной работы организации. Предложены различные меры для защиты информации в условиях дистанционного режима работы.

Ключевые слова: дистанционный режим работы, информационные технологии, корпоративные данные, удаленная работа, защита информации, информационная безопасность.

E.S. Ass [1]***, A.A. Butin*** [1]

[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

METHODOLOGICAL ASPECTS OF INFORMATION PROTECTION DURING REMOTE OPERATION OF THE ORGANIZATION

Annotation. The advantages and disadvantages of remote work, both for the employees themselves and for employers, are considered. The main risks of corporate data leakage in the mode of remote work of the organization are identified. Various measures have been proposed to protect information in the conditions of remote operation.

Key words: telecommuting, information technology, corporate data, remote work, information protection, information security.

Введение

В настоящее время происходит стремительный рост информационно-телекоммуникационных технологий. Быстрое развитие и внедрение информационных технологий позволило различным предприятиям и организациям модифицировать классическую форму трудовых отношений. Вследствие чего все большее распространение получил дистанционный режим работы, когда сотрудник выполняет трудовую функцию вне места нахождения работодателя.

Удаленный режим работы – это такой формат работы, который не подразумевает наличие сотрудника на территории работодателя. Удаленная работа позволяет выполнять рабочие обязанности из любого доступного места. Для сотрудников и предприятий такой формат работы является выгодным, поскольку и те и другие сокращают свои затраты на организацию рабочего процесса как прямо, так и косвенно.

Цифровизация бизнеса и использование современных информационных технологий позволяет бизнесу увеличивать свою эффективность и продуктивность за счет снижения временных издержек на взаимодействие между сотрудниками компании. Применение различных информационных технологий позволяет сотруднику банально экономить временные и финансовые ресурсы на дорогу в офис компании.

Удаленный формат работы для самих предприятий в свою очередь тоже позволяет экономить на обустройстве рабочих мест в офисах и возможности нанять большое количество сотрудников, не платя за увеличенную аренду и уборку большого офиса, электричество, канцелярию, и не тратить деньги на покупку мебели, офисной технички и т.д. К тому же компания может нанимать удаленных специалистов из регионов и таким образом экономить на зарплатах.

Текущий уровень информационных технологий позволяет работнику и работодателю не только связываться между собой на удаленном расстоянии в режиме реального времени, но и оперативно обмениваться результатами своего труда. Учитывая возможности

компьютерной техники и интернета, во многих случаях отпадает необходимость нахождения работника в офисе компании.

Однако, не смотря на все преимущества, такой формам трудовых отношений имеет и ряд значительных недостатков. Ведь на любом предприятии практически каждый сотрудник становится носителем ценных коммерческих сведений, которые представляют интерес для конкурентов. При дистанционном режим работы службы информационных технологий могут допустить различные ошибки и открыть доступ не тем сотрудникам к внутренней инфраструктуре компании, что в свою очередь в случае утечки корпоративных данных может привести к возникновению различных утечек и инцидентов информационной безопасности. В связи с этим возникает необходимость защиты информации предприятия.

С точки зрения компании сотрудник, работающий из дома, находится в ненадежной и неконтролируемой среде. Небрежное использование сотрудником корпоративных данных может привести к их утечке или краже. Для того, чтобы сотрудники осознали необходимость защиты корпоративной информации, необходимо регулярно и максимально в доступной форме информировать их, как правильно организовывать работу с корпоративными данными.

К тому же при дистанционном формате работы также возникает большое количество новых рисков. Поэтому для защиты корпоративных данных предприятия необходимо сформировать перечень рекомендаций для безопасной удаленной работы сотрудников, которые позволят максимально защитить корпоративную информацию компании.

Эта статья будет полезна тем организациям, которые функционируют в удаленном режиме работы и хотят защитить свои данные от утечки со стороны своих сотрудников [1, 2].

1. Достоинства и недостатки режима удаленной работы

В связи со стремительным развитием IT-технологий в мире становится все больше удаленных профессий. К тому же большая часть ведущих компаний уже давно принимает за норму дистанционный формат работы.

Удаленные сотрудники сейчас составляют почти 40% мировой рабочей силы, и эта цифра продолжает расти. Более того, целые компании переходят на удаленную работу, навсегда меняя физические пространства на онлайн-среду и используя кадровые ресурсы по всему миру ради развития бизнеса и сокращения расходов. Работа из любой точки и взаимодействие всех со всеми – таков офис будущего.

Безусловно, удаленная работа имеет свою специфику, а также преимущества и недостатки, как для сотрудников, так и для работодателей.

Главный страх руководства предприятий – это потерять контроль над корпоративными ресурсами, ведь использование личных устройств делает компанию уязвимее для атак киберпреступников, стремящихся завладеть самым ценным активом предприятии – её корпоративными данными.

Преимущества удаленной работы для сотрудника:

1) Экономия временных и финансовых затрат на дорогу до офиса. В больших городах дорога на работу и обратно может занимать 1-3 часа в день. Дорога в 3 часа по 20 рабочих дней в месяц каждый год занимает 720 часов в год, это примерно 30 дней в году. Это время, которое человек вычеркивает из своей жизни, вместо того чтобы делать что-то полезное. Но человек не занимается беспрерывно каким-либо делом в течение 24 часов, реальная продуктивность составляет 12 часов в день, получается, что 60 дней в году человек просто тратит на поездки на работу. Сейчас это время у многих появилось благодаря тому, что люди работают удаленном из дома, и могут потратить это свободное время на что-то еще. И наверняка очень многие люди не готовы с этим временем, которое у них появилось, просто так расставаться. То же самое касается и финансовых затрат сотрудников на дорогу до офиса и обеды, ведь не каждая компания имеет корпоративный транспорт для организации доставки всех сотрудников к месту работы и обратно.

2) Свободный и гибкий рабочий график. Основной задачей сотрудников заключается в выполнении заданий согласно их профессиональной деятельности. Ведь работая в офисе, можно хорошо поработать, и полностью сделать свой план дня, но это никого не волнует, сколько задач решено, ведь необходимо находится в офисе до конца рабочего дня. Работая удаленно, сотрудник не просто 8 часов находится в офисе, делая вид, что все 8 часов активно занимается выполнением своих должностных обязанностей. Сотрудник работает в удобном для него месте. И если он справляется с поставленным объемом задач за 4 часа, а не за 8, значит, у него останется больше времени на творчество, обучение, профессиональное общение, личную жизнь и повышение своих профессиональных навыков. Работник заинтересован в повышении производительности труда. Если кому-то удобнее работать днём, вечером или ночью, это не имеет никакого значения. Исключения составляют ситуации, когда сотрудник, например, выполняет обязанности менеджера по персоналу или работе с клиентами, когда ему необходимо связываться с людьми в строго определенное время. Удаленная работа повышает продуктивность и мотивированность сотрудников.

3) Нет привязки к определенному месту работу. Возможность осуществлять профессиональную деятельность из любой точки мира, одновременно путешествуя и работая удаленно. Сотрудник может выбирать рабочее место на свое усмотрение. Если ему комфортно, он работает из дома, а если желает сменить обстановку – идёт в кафе или коворкинг.

4) Совмещение работы и учебы. Удаленная деятельность экономит время, которое можно потратить на учебу. В особенности это касается онлайн-обучения, однако у работника есть возможность просто совместить очное обучение с утренней или вечерней работой.

5) Возможность самостоятельного планирования рабочего времени;

6) Удаленная занятость. Возможность трудоустройства для людей, которые живут в удаленных населенных пунктах, где нет большого разнообразия вакансий.

7) Можно работать даже когда сотрудник заболел. Работнику нет необходимости оформлять больничный лист и терять деньги, работая удаленно можно спокойно болеть и работать одновременно. То же самое, когда заболел кто-то из родственников работника.

8) Экономия на одежде. Сотруднику нет необходимости соблюдать дресс-код компании на удаленной работе. Работая из дома, работник может просто сидеть за компьютером в удобной домашней одежде и выполнять свои должностные обязанности.

Недостатки удаленной работы для сотрудника:

1) Трудности при организации профессиональной деятельности. Сфокусироваться на работе намного сложнее, если это происходит дома. Дело в том, что в таких условиях человек постоянно отвлекается на различные раздражители, поэтому сотруднику необходимо привить себе навык планирования и тайм-менеджмента. Кроме того, родные и близкие сотрудника живущие вместе с ним могут его постоянно отвлекать от рабочей деятельности. Офис в этом смысле куда более удобен.

2) Дефицит общения. Сотруднику может недоставать непосредственной коммуникации с коллегами. Кроме того, те работники, которые проживают одни, зачастую испытывают усиленную потребность в общении.

3) Переработка. Если у человека отсутствуют навыки тайм-менеджмента, то на удаленной работе время профессиональной деятельности может растянуться очень надолго из-за раздражительных факторов, которые будут отвлекать сотрудника от рабочей деятельности, для сотрудника создается ощущение работы 24/7.

4) Отсутствие удобного рабочего места. Не все сотрудники могут позволить себе отдельный кабинет для работы, и даже рабочий стол. Важно выделить рабочую зону, даже если жилое пространство очень маленькое.

5) Ограниченные возможности карьерного роста. Работая из дома, сотрудник не может по максимуму показать свои профессиональные навыки вышестоящему руководству, нежели работая в офисе.

6) Необходимость в высокоскоростном доступе в интернет для стабильного подключения к удаленные ресурсам, а также наличие высокопроизводительного средства вычислительной техники для комфортной работы.

Преимущества удаленной работы для работодателя:

1) Экономия затрат на оборудование офиса. Нет необходимости платить аренду за большой офис, коммунальные услуги, оборудовать рабочие места, покупать мебель и офисную технику, канцелярию и др. накладные расходы. Переход на удаленные режим работы также позволяет работодателю экономить и на косвенных расходах: обеспечение охраны, противопожарной безопасности, мелкие ремонты, затраты на зарплату обслуживающего персонала и т.д. Во многих современных компаниях есть практика компенсации оборудования рабочего места дома, обучения и покупки ПО. Очень часто эти компенсации полностью покрывают затраты работника. Но эти расходы даже близко не сопоставимы с содержанием классического офиса.

2) Неограниченный рынок труда для компании. Существует возможность нанять больше высококвалифицированных сотрудников из другого города или региона. Лучшие специалисты могут жить в другом городе, удаленная работа станет в этом случае отличным вариантом для сотрудничества. При таком увеличении выбора предприятия может выбрать специалистов лучшей квалификации, при лучших условиях оплаты труда. Снижение ФОТ за счет найма сотрудников в регионах.

3) Отсутствие проблем с контролирующими органами. Любая организация имеет дело с органами противопожарной безопасности, службой санитарно-эпидемического контроля и другими органами. При работе в дистанционном режиме нет необходимости различных разрешений от этих органов, никаких пропусков, каталогов инструктажей по безопасности и т.д. Нет офиса - нет проблем.

4) Производительность работников. Работники, имеющие высокий уровень самоорганизации и умеющие хорошо контролировать свой тайм-менеджмент, отключаются от отвлекающих внешних факторов и умеют выполнять свои должностные обязанности за более короткий срок, нежели сотрудники в офисе. Ведь длина его рабочего дня зависит от скорости достижения результата, а не от установленного работодателем времени. Офисные работники же наоборот быстро привыкают к восьмичасовому ограничению. В результате чего восьмичасовой рабочий день становится все менее производительным. Ведь зачем держать высокую интенсивность, если зарплата от этого не увеличится. Выбирая сотрудников, которые успешно работали удаленно, компания сильно повышает вероятность попасть на ответственного специалиста с высоким уровнем самоорганизации.

5) Результативность работы, повышение мотивации работника и IT культуры, лояльность сотрудника, возможность подстроиться под клиента, а не под фиксированный рабочий график;

6) Устойчивость к форс-мажорным обстоятельствам. В связи с различными политическими, экономическими, климатическими, эпидемиологическими факторами в стране работа компании в классическом офисном режиме может быть затруднена. Удаленный формат работы может помочь в этих ситуациях. Ведь невозможно придумать ситуацию, при которой людям законодательно запретят работать из дома. Предприятия, которые изначально заточены под удаленную работу, с такими проблемами не сталкиваются.

Недостатки удаленной работы для работодателя:

1) Требуются огромные инвестиции в технологии. Для комфортной удаленной работы компаниям приходится закупать дорогостоящие ноутбуки для сотрудников, ведь не у всех имеется домашний компьютер. К тому же для обеспечения информационной безопасности компаниям необходимо приобретать различные средства защиты информации.

2) Большие риски утечки информации при удаленной работе. Предприятия, которые перешли на удаленный режим работы несут огромные риски, т.к. сотрудники, которые работают удаленно забирают с собой в незащищенную домашнюю обстановку рабочие

документы. К тому же, неподготовленные сотрудники не знают всех правил обеспечения информационной безопасности при работе на удаленном режиме работы.

3) Отслеживание продуктивности сотрудников. Самая большая проблема, что далеко не все люди способны эффективно работать вне офиса. В домашней обстановке большой количество отвлекающих факторов, и сотрудник не может сконцентрироваться на рабочем процессе. К тому же, проблема отслеживания продуктивности также важно, ведь работодатель не может точно знать, чем именно сейчас занят сотрудник дома, выполняет профессиональные задачи, или гуляет с собакой на улице.

4) Низкое качество выполнения обязанностей и потеря объемов выполняемой работы. Работая из дома, сотрудник может большую часть своего времени посвящать не профессиональной деятельности, а своим домашним делам. И задачу, которую можно сделать, к примеру, за 1 час, сотрудник выполняет 3 часа, объясняя это тем, что случился форс-мажор, либо он не сразу нашел решение и т.д. В таком случае руководитель должен отслеживать таких сотрудников, оценивать задачи и контролировать эффективность их выполнения.

5) Нехватка очного общения с сотрудниками по рабочим вопросам.

6) Проблемы с обратной связью. Иногда сотрудник при необходимости не всегда может быть на связи и не сможет взять в работу срочное задание, либо просто не сможет ответить при звонке по каким-либо причинам или намерено. А причин может быть просто огромное количество: сотрудник на обеде, ушел гулять, решил принять душ и т.д. Либо просто потерял телефон или ноутбук. Необходимо обговаривать такие моменты с сотрудниками, чтобы телефон в рабочее время всегда был при себе.

Несмотря на все преимущества и недостатки, удаленная работа, как для сотрудников, так и для предприятий выгодна и эффективна. Но необходимо потратить большое количество временных и финансовых ресурсов на отладку всех бизнес-процессов организации и на обеспечение должного уровня информационной безопасности [3, 4].

2. Основные риски утечки корпоративных данных при организации удаленной работы

Резкий переход на удаленный режим работы испытали на себе очень многие компании. Они оперативно перестраивали свой бизнес, пытаясь сохранить эффективность и при этом уберечься от новых угроз и рисков при организации удаленной работы сотрудников.

При работе сотрудников вне офиса возникает риск кражи данных компании и увеличения количества угроз информационной безопасности.

Учитывая скорость перехода предприятий на удаленный режим работы, процессы обеспечения информационной безопасности были нарушены, резко выросли риски, которые могли в принципе отсутствовать при обычном режиме работы бизнеса.

Работа сотрудников из дома связана с отсутствием достаточного контроля, что провоцирует большое количество новых рисков в плане информационной безопасности.

К числу рисков информационной безопасности, связанных с удаленной работой, относятся: ошибки в идентификации и аутентификации пользователей, фишинговые атаки, взлом маршрутизаторов и перенаправление пользователей на вредоносные сайты, несанкционированный доступ к корпоративным ресурсам из-за пределов периметра безопасности, нарушение конфиденциальности информации при ее передаче по открытым каналам связи и др.

В связи с массовым переводом сотрудников на удаленную работу значительно повышаются шансы проведения успешных кибератак на предприятия, поскольку уровень защиты домашнего компьютера сотрудника с большой долей вероятности значительно ниже, чему корпоративного рабочего места. К тому же домашние сети защищены гораздо слабее, чем сети организаций, что делает подключенные к ним компьютеры источником серьезных потенциальных проблем. К числу рисков информационной безопасности, связанных с

удаленной работой относится модификация трафика, перехват конфиденциальных данных и паролей, взлом маршрутизаторов и перенаправление пользователей на вредоносные сайты.

Поскольку не все компании имеют возможность снабдить своих сотрудников служебным компьютером, тогда работник вынужден использовать личное устройство, нередко это может быть домашний компьютер, которым пользуется сразу несколько членов его семьи, что влечет за собой множество рисков.

В первую очередь, это риски, связанные с заражением вредоносным программным обеспечением. Они могут привести к потере данных, проникновению во внутреннюю инфраструктуру компании и в результате нарушению работы всей корпоративной сети. Заражение вредоносным программным обеспечением может привести и к потере личных данных, если для работы используется домашний компьютер. В качестве основного варианта реализации рисков можно рассматривать социальную инженерию. Злоумышленники могут придумывать изощренные способы получения несанкционированного доступа к чувствительной корпоративной информации, имитировать письма и звонки сотрудников технической поддержки с просьбой выслать логины и пароли от рабочих учетных записей. Учитывая, что работа из дома в разы увеличивает число коммуникаций через незащищенную электронную почту и мессенджеры, это повышает риски успешной реализации подобных атак.

При переходе на удаленку усилился риск утечки данных при атаке извне, когда сотрудник работает со своего компьютера. Это значительно упрощает злоумышленникам как кражу корпоративных данных, так и проникновение во внутреннюю сеть компании. К тому же персональные компьютеры всех удаленных сотрудников намного сложнее контролировать за пределами офиса.

Ранее, если сотрудник допускал ошибку и попадался, например на фишинг, то другие системы обеспечения информационной безопасности организации могли его подстраховать. При попытке отправить конфиденциальную информацию могла сработать DLP система, при попытке получить доступа к зараженному файлу мог отработать антивирус и т.д. Теперь же ответственность за значительную часть информационной безопасности была перенесена с систем защиты организации на пользователя.

Злоумышленники активно используют электронную почту для распространения фишинговых ссылок и вредоносных программ во вложениях и эффективность их достаточно высока, так как пользователи, получая и вполне легальные новостные рассылки, не всегда в общем объеме могут распознать и что-то вредоносное. К тому же у сотрудников возникают идеи обмена корпоративной критической информацией через облачные системы или использование домашнего незащищенного ПО для служебных целей. Из-за того, что в большинстве случаев переход на удаленку был экстренный – большинство сервисов просто физически не успели нормально настроить.

Один из главных рисков удаленной работы – инсайдерская активность. В режиме удаленной работы она возрастает многократно. С технической стороны дистанционная работа стала проблемой для компаний, которые раньше не работали в таком формате и переходили на такой режим работы в сжатые сроки. Типичные ошибки, которые могут допустить компании – это слабая защищенность канала удаленного подключения, не настроенная двухфакторная аутентификация, даны избыточные доступы к корпоративным ресурсам. В итоге трафик удаленных сессий могут перехватить злоумышленники, а сотрудники получат в распоряжение конфиденциальные данные, работать с которыми по должности им не положено. Плюс ко всему, не у всех предприятий хватит мощностей, чтобы поддержать стабильную работу корпоративных ресурсов при массе удаленных подключений.

Отдельный вопрос – это получение доступа к корпоративной сети – даже при утрате логина и пароля пользователя возможен ограниченный доступ с использованием удаленного подключения. Но сейчас удаленные подключения разрешены и системы ИБ, которые раньше страховали пользователей, не выполняют своих функций, и ответственность за информационную безопасность лежит полностью на пользователе.

Большая часть компаний не была готова к переходу на удаленную работу: в дистанционном режиме работы оказалось практически невозможно контролировать действия сотрудников. Многие из них получили потенциальную возможность безнаказанно разглашать конфиденциальные данные, в том числе с использованием личной техники (скриншоты, фотографирование экрана или распечатывание документов на домашнем принтере). Проблема заключается в том, что большинство существующих ИТ-решений на рынке пока не способны бороться с этой угрозой и получается, что ответственность за информационную безопасность лежит полностью на сотруднике.

Стоит отметить, что возможности украсть данные либо вывести их из компании были доступны и раньше: все рабочие компьютеры давно подключены к сети, а сотрудники используют в работе свои собственные смартфоны, которые никто и никак не контролирует.

В связи с переходом многих сотрудников на удаленную работу на первый план выходят риски, связанные с:

– хранением и управлением данных в облачных хранилищах;

– утечкой и кражей данных и потерей мобильных устройств или средств вычислительной техники;

– утечкой и перехватом аутентификационных данных;

– несанкционированным доступом к информационным системам;

– заражением устройства вредоносным ПО, с которого осуществляется удаленный доступ к корпоративным информационным ресурсам;

– передачей техники в ремонт;

– несанкционированным доступом к рабочему устройству родных и знакомых;

– устаревшими устройствами веб-защиты;

– устаревшими механизмами удаленного доступа.

Необходимо рассматривать риски с точки зрения появления новых сценариев и проводить переоценку рисков в связи с увеличением вероятности событий.

Так, если в компании отсутствует электронный документооборот или применяется от случая к случаю, могут возникнуть риски не получить своевременно доступ к информации, например, к договорам с клиентами, операционным планам и записям, которые хранятся в виде бумажных документов в офисе.

Массовый переход на системы для онлайн-конференций выявили их уязвимости — а именно отсутствие должной защиты конфиденциальных данных, что может представлять угрозу для организаций. Конфиденциальность также подвержена новым рискам: ведь данные, с которыми работают сотрудники в домашних условиях, с большей вероятностью могут быть раскрыты посторонним лицам.

Может нарушиться и целостность информации – она может быть повреждена и изменена из-за незнания сотрудниками новых инструментов, с которыми им пришлось работать вне офиса.

Если к переходу на удаленную работу организация не обеспечила достаточное количество ресурсов для обеспечения средств хранения информации (серверов, облачной среды), а также не внедрила меры по защите хранящейся информации, не провела обучение сотрудников, могут возникнуть риски для:

– целостности информации (она может быть по ошибке изменена);

– конфиденциальности (такая система не обеспечивает защиту от несанкционированного доступа);

– доступности (сотрудники не могут получить доступ к нужным документам удаленно).

Таким образом, изменение контекста и процессов компании при переходе на удаленную работу требует пересмотра рисков, связанных с информационной безопасностью.

3. Защита корпоративных данных при удаленной работе сотрудников

При удаленной работе на первый план выходит безопасность конечных устройств, а прежняя концепция периметра, который нужно защищать, устарела. Именно с этой точки зрения следует оценивать способы обеспечения информационной безопасности сейчас. Необходимо произвести пересмотр существующих организационно-технических механизмов обеспечения информационной безопасности в организации и на предприятии.

Для защиты корпоративных данных предприятия необходимо максимально обеспечить защиту устройств сотрудников, на которых они работают из дома. Для защиты необходимо использовать безопасное VPN-соединение и многофакторную аутентификацию, системы защиты от утечек (DLP) и системы контроля привилегированных пользователей (PIM/PAM).

1) Решения для безопасного VPN-подключения.

Наиболее актуальны для всех компаний в режиме удаленной работы стали решения для защиты каналов связи, по которым происходит обмен информацией. В основе этих решений – программные и программно-аппаратные VPN-продукты.

Необходимо, чтобы пользователь мог легко получить доступ в корпоративную сеть с любого доверенного устройства и при использовании любой операционной системы, а администратор информационной безопасности всегда понимал состояния этого устройства. Действенным способом решения задачи по защите обмена данными между офисом и удаленными сотрудниками является использование собственного VPN-сервера в сети компании. VPN-туннелирование в сочетании с настроенной матрицей доступа позволило многим компаниям быстро перейти на удаленный режим работы, сохранив разграничение прав доступа к корпоративным информационным системам.

2) Средства многофакторной аутентификации.

Удаленный доступ повышает спрос на технологии многофакторной аутентификации. Такая аутентификация с использованием сертификатов, токенов (физических или программных) и с верно настроенными групповыми политиками решает проблему несанкционированного доступа к информации. Ведь стандартная пара логин-пароль уже давно считается небезопасной, в особенности при аутентификации на корпоративном ресурсе, доступным из сети Интернет. В то же время VPN не всегда удобен для обычных пользователей, поэтому IT-службы обеспечивают возможность сотрудниками обращаться к корпоративным сервисам без VPN, что требует более надежной аутентификации, позволяющей работать как с компьютеров, так и с мобильных устройств. Возрос интерес к средствам аутентификации, в частности двухфакторной аутентификации с помощью USB-токенов, смарт-карт или SMS-сообщением с кодом авторизации. С помощью данных средств реализуется двухфакторная аутентификация к защищаемым данным на ноутбуках и стационарных ПК.

3) Средства контроля утечек информации и продуктивности сотрудников.

В период массового перевода компаний на удаленный режим работы увеличился спрос на системы для защиты от утечек информации (DLP, Data Leak Prevention) и специализированные решения для удаленного мониторинга активности сотрудников. DLP-системы позволяют контролировать рабочие места вне офиса и предотвращать утечки конфиденциальной информации из внутреннего периметра сети, даже если рабочая сеть и ее сегменты распределены географически. Причина использования систем контроля продуктивности сотрудников проста – работодатели хотят знать, чем сотрудники заняты вне их поля зрения. Средства контроля действий сотрудником используется скорее не для решения задач ИБ, а для контроля удаленных сотрудников, чтобы удостовериться действительно ли они работают.

4) Системы контроля привилегированных пользователей.

Удаленный доступ всегда был большой проблемой для сотрудников на удаленке, но когда дистанционно работают люди у которых привилегированные права администратора систем и доступы к базам данным и домена это многократно увеличивает уровень угроз. Переход на удаленный режим работы дал толчок развития системам контроля за

привилегированными пользователями и системам управления и контроля доступа, т.к. необходимо наблюдать, что администраторы делают с серверами, а сотрудники с привилегированным доступом к критичным бизнес-системам. Многие администраторы информационных систем перешли на удаленную работу и стали выполнять свои функции с домашних компьютеров и дополнительный рубеж защиты в виде системы контроля действий привилегированных пользователей стал крайне актуальным.

5) Продукты для защиты веб-приложений.

Увеличившееся количество дистанционных работников и миграция в онлайн способствовало необходимости публикации корпоративных сервисов в качестве веб-приложений. Вследствие чего востребованными стали продукты для защиты веб-приложений (WAF). Сейчас наиболее опасными становится угрозы, которые могут нарушить работоспособность интернет ресурсов компании и привести к остановке рабочих процессов – будь то внутренний документооборот, корпоративные коммуникации или онлайн-продажи. Растет и зависимость компаний от тех или иных информационных ресурсов, которые она использует в работе, поэтому особенно важно становится заботиться об их доступности информационной безопасности. Таким образом, наиболее актуальными сервисами для безопасной удаленной работы, стали защита от DDoS-атак и защита веб-приложений от злоумышленников.

6) Облачные защитные решения.

При срочном перехода на удаленный формат работы бизнес столкнулся с новыми нагрузками на ИТ инфраструктуру. Даже технологически развитые компании были вынуждены перераспределять мощности, чтобы обеспечить работоспособность своих корпоративных ресурсов при множестве удаленных подключений. Но технических мощностей ресурсов при резко возросшей нагрузке может не хватать под решения информационной безопасности, и поэтому предприятия стали обращаться за аутсорсингом и вендорам за облачными защитными решениями в области информационной безопасности. Такие решения позволяют предприятиям хорошо сэкономить на единовременной закупке дорогостоящего оборудования и ресурсозатратного ПО, а оплачивать подписку на облачные защитные решения помесячно.

7) Модель защиты нулевого доверия.

При дистанционном формате работы компании становится актуальна модель защиты нулевого доверия (zero trust). Она предполагает выстраивание подходов к защите, основываясь на полном отсутствии доверия к любым пользователям, подключающимся к корпоративным ресурсам. Пользователи и устройства должны каждый раз подтверждать свою подлинность при подключении к ресурсам. Ведь сотрудники могут подключаться в корпоративную сеть из любого места и с любого персонального устройства и контроль за этими устройства по умолчанию практически отсутствует, а значит доверять им невозможно. При построении системы защиты предприятия рекомендуется применять решения и технологии, которые обеспечивают реализацию принципов zero trust: многофакторная аутентификация, которая позволяет защититься от скомпрометированных паролей сотрудников, проверки устройств сотрудников на наличие установленных обновлений, актуальность антивирусных баз, шифрование данных на устройствах сотрудников для защиты и др.

8) Другие технологии защиты удаленных рабочих мест.

При организации удаленной работы многие компании был сконцентрированы на решениях для безопасного удаленного доступа: VPN-шлюзы, решения для многофакторной аутентификации, PAM решения и т.п. Но достаточно быстро предприятия поняли, что этого недостаточно для поддержания бизнес-процессов. В результате спрос пошел в сторону комплексных решений, обеспечивающих безопасную работу с чувствительной информацией и объединяющих в себе технологии VPN, защиту удаленных рабочих мест от НСД, систему двухфакторной аутентификации, трансформацию системы мониторинга информационной безопасности, а также при необходимости шифрование ГОСТ. Такие системы позволяют раз

и навсегда отказаться от стационарного рабочего места в пользу терминальной станции, и позволяет организовать в любой момент времени защищенный удаленный доступ любому количеству работников без дополнительных действий со стороны обслуживающего персонала, а также исключить утечки конфиденциальной информации путем запрета передачи вовне любой информации, кроме графической (средствами VDI). Кроме того, это повысит надежность механизмов аутентификации и позволит получить гибкую возможность горизонтального и вертикального масштабирования в любой момент времени. Но следует также понимать, что универсальной программы для закрытия всех задач не существует, и многое зависит от инфраструктуры конкретного предприятия и его бизнес-процессов.

Также актуальными стали средства для управления мобильными устройствами и системы класса EDR, ведь обращаться к корпоративным ресурсам с не доверенных устройств это большой риск. MDM и EDR системы позволяют снизить эти риски и повысить уровень доверия к устройствам, с которых сотрудники обращаются к корпоративным ресурсам.

Вместе с тем набирают популярность продукты, которые обеспечивают возможность безопасной работы сотрудника в не доверенной среде. Например, средства шифрования информации на ноутбуках дистанционных работников (Secret Disk), различные межсетевые экраны и сканеры (ПАК «Рубикон»), комплексы средств анализа защищенности («Сканер-ВС») и системы управления событиями информационной безопасности («КОМРАД»).

При удаленной работе для обмена корпоративными данными сотрудникам нежелательно использовать корпоративный мессенджер, лучше обмениваться данными через защищенный почтовый клиент с антиспам-защитой, предварительно отправляемую информацию поместив в архив и защитить паролем. Пароль сообщить получателю либо по телефону, либо передать его в другому корпоративном мессенджере. Этот способ является альтернативным безопасным методом передачи информации при отсутствии других средств защиты.

Однако основная роль в обеспечении защищенности корпоративных данных при удаленной работе все же лежит на самих сотрудниках предприятия, которые либо будут соблюдать инструкции, правила и требования по информационной безопасности, либо нет. Второстепенную роль занимают подразделения, обеспечивающие поддержку информационной безопасности инфраструктуры предприятия.

В последнее время в связи с различными инцидентами информационной безопасности доверие к иностранным продуктам значительно снизилось, вследствие чего возрос интерес в первую очередь к отечественным решениям. Причин тому несколько: стоимость, доверие и требования законодательства по импортозамещению.

Таким образом, потребность в решениях информационной безопасности определяется целями и задачами, которые ставит перед собой сама компания. Для этого в первую очередь необходимо сделать анализ, определить свою политику безопасности и провести оценку новых технологий на предмет их применимости для предприятия [5, 6, 7].

Заключение. Дистанционный режим работы организации может привести как к утечке корпоративных данных, так и к нарушению работы целых функциональных систем предприятий вследствие неосторожности самих сотрудников, а также в случае кражи или утечки корпоративной информации не по их вине.

Используя все вышеперечисленные меры по защите корпоративных данных, можно избежать большинства угроз, рисков и инцидентов, связанных с информационной безопасностью корпоративных данных предприятия.

К тому же, при уменьшении количества недостатков удаленного режима работы, как для сотрудников, так и для работодателей, возможно будет сконцентрироваться только на преимуществах и тем самым обеспечить более быструю адаптацию сотрудников и более высокую трудовую эффективность, что в конечном итоге скажется на более высокой производительности сотрудников предприятия, что в конечном итоге приведет к увеличению чистой прибыли компании.

Подводя итоги, можно сказать, что контролировать действия сотрудников на удалённых рабочих местах необходимо не только с точки зрения обеспечения безопасности, но и с позиций эффективности бизнес-процессов. Однако в желании не потерять контроль над компанией, защитить конфиденциальные данные от утечек и отладить рабочие процессы в этот непривычный для всех период важно помнить, что бизнес строится на людях. И если за ними неустанно следить, то лояльность и желание приносить пользу компании будут неуклонно снижаться, а количество умышленных утечек — наоборот, расти.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Базаров Р.С. Удаленная работа как новая реальность // Журнал «Трибуна ученого». – 2020. – №11. – С. 14-18.

2. Босова Е.Д. Селищев В.А. Информационная безопасность: современные реалии // Известия Тульского государственного университета. Технические науки. Вып. 9. – 2020. – С. 296-300.

3. Бутин А.А., Василевская А.Н. Обзор основных рекомендация по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции // Информационные технологии и математическое моделирование в управлении сложными системами. Иркутск: ИрГУПС. – 2020. – №2 (7). – С. 39-45.

4. Иванченко А.А., Бутин А.А. Использование DLP-систем при расследовании инцидентов информационной безопасности // Информационные технологии и проблемы математического моделирования сложных систем. Иркутск: ИрГУПС. – 2017. – № 18. – С. 15-22.

5. ISO 27001 и риски информационной безопасности при переходе на удаленную работу [Электронный ресурс]. – Режим доступа: https://www.sgs.ru/ru-ru/news/2020/04/iso-27001-i-riski-informacionnoj-bezopasnosti-pri-perehode-na-udalennuyu-rabotu. – Заглавие с экрана. – (дата обращения: 25.05.2022).

6. Как защитить корпоративные данные при удаленной работе [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/management/blogs/2020/06/08/832180-zaschitit-korporativnie. – Заглавие с экрана. – (дата обращения: 25.05.2022).

7. Носков С.И., Бутин А.А. Методическое обеспечение оценки уровня уязвимости объектов информатизации // Информационные технологии и проблемы математического моделирования сложных систем. Иркутск: ИрГУПС. – 2015. – № 14. - С. 38-48.

REFERENCES

1. Bazarov R.S. Remote work as a new reality // Journal "Scientist's Tribune". - 2020. - No. 11. - S. 14-18.

2. Bosova E.D. Selishchev V.A. Information security: modern realities // Bulletin of the Tula State University. Technical science. Issue. 9. - 2020. - S. 296-300.

3. Butin A.A., Vasilevskaya A.N. Overview of the main recommendations for the prevention of information security incidents in conditions of remote work and self-isolation // Information technologies and mathematical modeling in the management of complex systems. Irkutsk: IrGUPS. - 2020. - No. 2 (7). - S. 39-45.

4. Ivanchenko A.A., Butin A.A. The use of DLP-systems in the investigation of information security incidents // Information technologies and problems of mathematical modeling of complex systems. Irkutsk: IrGUPS. - 2017. - No. 18. - P. 15-22.

5. ISO 27001 and information security risks in the transition to remote work [Electronic resource]. – Access mode: https://www.sgs.ru/ru-ru/news/2020/04/iso-27001-i-riski-informacionnoj-bezopasnosti-pri-perehode-na-udalennuyu-rabotu. - Screen title. – (date of access: 05/25/2022).

6. How to protect corporate data when working remotely [Electronic resource]. – Access mode: https://www.vedomosti.ru/management/blogs/2020/06/08/832180-zaschitit-korporativnie. - Screen title. – (date of access: 05/25/2022).

7. Noskov S.I., Butin A.A. Methodological support for assessing the level of vulnerability of informatization objects // Information technologies and problems of mathematical modeling of complex systems. Irkutsk: IrGUPS. - 2015. - No. 14. - S. 38-48.

Информация об авторах

Евгений Сергеевич Асс – студент гр. БИм.1-20-1, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: evgeniyirk98@mail.ru

Александр Алексеевич Бутин – доцент кафедры «ИСиЗИ», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

Authors

Evgeny Sergeevich Ass – student gr. BIm.1-20-1, Irkutsk State Transport University, Irkutsk, e-mail: evgeniyirk98@mail.ru

Alexander Alekseevich Butin – Associate Professor of the Department of ISIS, Irkutsk State University of Railways, Irkutsk, e-mail: butin_aa@mail.ru

Для цитирования

Асс Е.С., Бутин А.А. Методические аспекты защиты информации при дистанционном режиме работы организации // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №2(14). – С.65-76– DOI: 10.26731/2658-3704.2022.2(14).65-76 – Режим доступа: http://ismm-irgups.ru/toma/214-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 30.06.2022)

For citation

Ass E.S., Butin A.A. Methodological aspects of information security in the remote mode of operation of the organization. [Electronic resource] // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 2(14). P. 65-76. DOI: 10.26731/2658-3704.2022.2(14).65-76 [Accessed 30/06/22]