УДК 004.056.5

Е.С. Асс [1]***, А.А. Бутин*** [1]

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

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ МАССОВОГО ПЕРЕВОДА СОТРУДНИКОВ НА УДАЛЕННУЮ РАБОТУ

Аннотация. Статья посвящена вопросам обеспечения информационной безопасности предприятия в условиях массового перевода сотрудников на удаленную работу. Рассмотрено нормативное регулирование вопроса дистанционной работы. Определены основные угрозы информационной безопасности при работе в удаленном режиме. Описаны четыре подхода по переводу сотрудников предприятия на удаленную работу. Предложены различные рекомендации по минимизации рисков предприятия при переводе сотрудников на удаленную работу.

Ключевые слова: информационная безопасность, дистанционный режим работы, удаленная работа, удаленный доступ, корпоративная информационная система предприятия.

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

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

ISSUES OF ENSURING THE INFORMATION SECURITY OF THE ENTERPRISE UNDER THE CONDITIONS OF MASS TRANSFER OF EMPLOYEES TO REMOTE WORK

Annotation. The article is devoted to the issues of ensuring information security of an enterprise in the conditions of mass transfer of employees to remote work. The normative regulation of the issue of remote work is considered. The main threats to information security when working in remote mode have been identified. Four approaches are described for transferring employees of an enterprise to remote work. Various recommendations are proposed for minimizing enterprise risks when transferring employees to remote work.

Key words: information security, remote operation, remote work, remote access, corporate information system of an enterprise.

Введение

В условиях массового и быстрого перехода в режим самоизоляции, государство вынудило предприятия различных сфер деятельности оперативно предоставить своим сотрудниках удаленный доступ к корпоративным ресурсам и системам, который им необходим для выполнения своих трудовых обязанностей.

На сегодняшний день большинство предприятий не готовы к такому быстрому переходу, так как, к сожалению, не во всех сферах деятельности возможно удаленно работать. Однако возможно полностью или частично перевести на удаленную работу до 40% от общего числа людей работающих на предприятии. К тому же при переводе сотрудников на удаленную работу многие предприятия столкнулись с достаточно серьезной проблемой, связанной с обеспечением сотрудников необходимыми ресурсами и данными для работы. Сам переход на дистанционный режим работы требует некоторого времени, наличия ресурсов и адаптации сотрудников к новому порядку работы.

Удаленный режим работы пользуется особой популярностью у следующих профессий (рис. 1) [8].

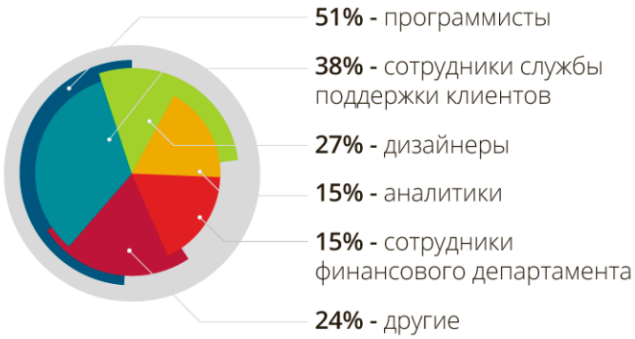

Рис. 1. Профессии с дистанционной занятостью

При массовом переводе сотрудников на дистанционный режим работы из других сфер деятельности соотношение профессий может сильно измениться. К тому же по данным опроса, лишь 20% компаний контролируют рабочий день дистанционных сотрудников [8].

Помимо очевидных проблем и недостатков, которые несет удаленная работа, существуют и другие, которые менее очевидны, однако несут за собой гораздо больше рисков и угроз, а именно угрозы информационной безопасности.

При выполнении своих трудовых обязанностей сотрудник обычно использует рабочий компьютер, который находится на территории предприятия и подключен к корпоративной информационной системе предприятия. Как правило, организации и предприятия обеспечивают тот или иной уровень защищенности корпоративной сети, а также самого компьютера сотрудника. Также в крупных компаниях существует отдел информационных технологий, или отдел информационной безопасности, или же просто отдел безопасности, функции которого предотвращение не только внешних атак и инцидентов, но и внутренних, например, угроз разглашений коммерческой тайны или распространения персональных данных [2]. Домашние же сети защищены гораздо слабее, чем сети организации, что делает подключенные к ним компьютеры источником больших рисков. К числу рисков информационной безопасности, связанных с удаленной работой, относится модификация трафика, перехват паролей и конфиденциальных данных, а также взлом маршрутизаторов и перенаправление пользователей на вредоносные сайты. Помимо этого, недобросовестные сотрудники при удаленной работе могут не качественно или не в полной мере выполнять свои обязанности, тем самым принося моральный или финансовый ущерб компании [1].

Вследствие чего появилась необходимость сформировать регламент предоставления сотрудникам удаленного доступа к ресурсам корпоративной сети с помощью различных специализированных программно-технических средств, позволяющих обеспечивать приемлемый уровень безопасности данных.

С течением времени обнаружилось, что при переходе на режим дистанционной работы организационные и технические меры политики информационной безопасности предприятия сильно отстают от действительности. Возник вопрос о необходимости обеспечения безопасности, как самих корпоративных сетей, так и данных, циркулирующих в них за пределы локальной сети компании.

Эта статья будет полезна тем владельцами предприятий, которые оказались в такой ситуации и хотят защитить свои корпоративные данные от утечки в условиях перехода на дистанционный режим работы.

1. Нормативное регулирование вопроса дистанционной работы

Возможность использования труда удаленных сотрудников появилась еще в 2013 году, нормативное регулирование такого формата трудовых отношений и само понятие предусмотрено Главой 49.1 Трудового кодекса Российской Федерации «Особенности регулирования труда дистанционных работников». Согласно нему: Дистанционной (удаленной) работой (дистанционная работа) является выполнение определенной трудовым договором трудовой функции вне места нахождения работодателя, его филиала, представительства, иного обособленного структурного подразделения, вне стационарного

рабочего места, территории или объекта, прямо или косвенно находящихся под контролем работодателя, при условии использования для выполнения данной трудовой функции и для осуществления взаимодействия между работодателем и работником по вопросам, связанным с ее выполнением, информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей связи общего пользования. Трудовым договором или дополнительным соглашением к трудовому договору может предусматриваться выполнение работником трудовой функции дистанционной на постоянной основе (в течение срока действия трудового договора) либо временно (непрерывно в течение определенного трудовым договором или дополнительным соглашением к трудовому договору срока, не превышающего шести месяцев, либо периодически при условии чередования периодов выполнения работником трудовой функции дистанционно и периодов выполнения им трудовой функции на стационарном рабочем месте) [4].

При заключении трудового договора о дистанционной работе в его условиях можно предусмотреть обязанность использования работником предоставленных или рекомендованных работодателем программно-технических средств, оборудования, а также средств защиты информации и иных средств.

Важно понимать, что обеспечение информационной безопасности предприятия полностью лежит на его руководителе. Поэтому на любом предприятии, где есть необходимость защищать корпоративные ресурсы, базы данных, финансовые документы, персональные данные сотрудников, обязательно и необходимо ввести режим коммерческой тайны и ознакомить с ним всех работников под подпись.

2. Основные подходы перевода сотрудников предприятия на удаленную работу

Многие предприятия для удешевления перехода на удаленный режим работы ошибочно отталкиваются только от возможных затрат на приобретение уже готовых продуктов и решений, которые преимущественно рассчитаны на быстрое и дешевое внедрение, которые в свою очередь имеют в своем составе только базовый (минимальный) набор средств защиты или не имеют его вообще. Равным образом будет являться ошибкой и использование личных устройств сотрудников: домашнего персонального компьютера, планшетов и смартфонов, с установленным на них стандартного программного обеспечения, в том числе антивирусного, а также использование сотрудниками личной электронной почты. Такое отношение работодателя к дистанционному режиму работы имеет наибольшие риски и уязвимости, так как личные устройства сотрудников, как правило, очень слабо защищены от взлома, а порой и вовсе не защищены, что в свою очередь очень сильно скажется на безопасности корпоративных данных и ресурсов компании.

Поскольку задача перехода на удаленную работу предполагает целый комплекс организационно-технических мер, то для построения защищенных каналов связи и работы с данными и документами без их утечки приводит к существенной перестройке процессов защиты информации.

Согласно данным из разных источников, 70-80% сотрудников работающих удаленно используют для работы свои домашние компьютеры или ноутбуки. Как уже отмечено ранее, использование личных средств вычислительной техники в качестве устройств для удаленной работы недопустимо, поскольку это несет очень большие риски и уязвимости для корпоративных данных.

Рассмотрим основные подходы по переводу сотрудников предприятия на удаленную работу:

1) использование личного устройства сотрудника, без подключения к общей корпоративной сети;
2) использование личного устройства сотрудника, с подключением к общей корпоративной сети тем или иным способом;
3) использование рабочего компьютера, находящегося дома у сотрудника без подключения к корпоративной сети и установки дополнительных средств защиты;

4) использование рабочего компьютера, который находится у сотрудника с подключением к общей информационной системе предприятия и другим корпоративным сервисам с установленными дополнительными средствами защиты.

Первый подход является самым дешевым и простым для предприятия, поскольку задействуется минимум финансовых средств и усилий со стороны работодателя для перевода сотрудников на удаленную работу. Однако одновременно с этим этот способ несет множество недостатков и содержит в себе большое количество рисков и уязвимостей:

– отсутствие возможности контроля деятельности сотрудника со стороны работодателя;

– при отсутствии специального программного обеспечения сотрудник не сможет выполнять некоторую часть своих обязанностей;

– многих сотрудников нельзя перевести на удаленную работу, поскольку их трудовые обязанности требуют либо личного присутствия, либо необходимо подключение к корпоративной информационной системе или другим локальным сервисам предприятия;

– присутствуют риски распространения сотрудником конфиденциальной информации;

– угроза безнаказанно копировать конфиденциальные данные, в том числе, с использованием личной техники (скриншоты, фотографирование экрана или распечатанных документов на смартфон);

– отсутствие контроля за устанавливаемым программным обеспечением;

– выход в сеть через незащищенные соединения;

– есть риски невыполнения требований законодательства в области информационной безопасности и политики информационной безопасности предприятия;

– не все сотрудники дома имеют личное устройство для удаленной работы.

Второй подход является более сложным для осуществления, так как требует от работодателя больше временных и финансовых затрат и есть необходимость подключения к корпоративной информационной сети предприятия, однако он также имеет уязвимости и угрозы:

– присутствуют угрозы заражения рабочего компьютера и корпоративной информационной системы при обмене файлами между домашним и рабочим устройством;

– многих сотрудников нельзя перевести на удаленную работу, поскольку их трудовые обязанности требуют личное присутствие;

– есть риски информационных инцидентов из-за несоблюдения правил и инструкций по удаленной работе;

– риски копирования и похищения коммерческой тайны и персональных данных на внешний носитель;

– отсутствие контроля за устанавливаемым программным обеспечением;

– выход в сеть через незащищенные соединения;

– угроза безнаказанно копировать конфиденциальные данные, в том числе, с использованием личной техники (скриншоты, фотографирование экрана или распечатанных документов на смартфон);

– не все сотрудники дома имеют личное устройство для удаленной работы.

Третий подход требует от работодателя уже более существенных финансовых и временных затрат, поскольку необходимо приобрести рабочую технику для каждого сотрудника, который будет работать в дистанционном режиме, однако, в нём также присутствуют риски, только другие:

– риск похищения или замены комплектующих рабочего компьютера;

– риски заражения рабочего компьютера;

– отсутствие возможности контроля деятельности сотрудника со стороны работодателя;

– угрозы заражения рабочего компьютера;

– риски копирования и похищения коммерческой тайны и персональных данных на внешний носитель;

– риски распространения конфиденциальной информации;

– многих сотрудников нельзя перевести на удаленную работу, поскольку их трудовые обязанности требуют либо личного присутствия, либо необходимо подключение к корпоративной информационной системе или другим локальным сервисам предприятия;

– присутствуют риски невыполнения требований законодательства в области информационной безопасности и политики информационной безопасности предприятия.

Четвертый подход перекрывает большинство рисков, однако является наиболее сложным и трудозатратным для предприятия, так как требует от работодателя большие финансовые и временные затраты для обеспечения должного уровня безопасности рабочего компьютера, но он также несёт в себе некоторые угрозы и недостатки:

– многих сотрудников нельзя перевести на удаленную работу, поскольку их трудовые обязанности требуют личное присутствие;

– есть угрозы информационных инцидентов из-за несоблюдения правил и инструкций по удаленной работе;

– риски копирования и похищения конфиденциальной информации посредством фото-видеосъемки экрана устройства;

– есть риски невыполнения требований законодательства в области информационной безопасности и политики информационной безопасности предприятия [1].

Таким образом, рассмотрев недостатки, уязвимости, угрозы и риски различных подходов организации удаленного рабочего места, можно отметить, что дистанционный режим работы наиболее подвержен рискам. Так как в дистанционном режиме работы оказалось практически невозможно контролировать действия сотрудников и существуют угрозы копирования и похищения конфиденциальной информации с личного или рабочего устройства посредством фото-видеосъемки и угрозы несоблюдения сотрудником правил и требований законодательства информационной безопасности и политики информационной безопасности предприятия.

3. Рекомендации по минимизации рисков предприятия при удаленном режиме работы

Правильным подходом работодателя для обеспечения информационной безопасности предприятия и корпоративных данных является соблюдение следующих рекомендаций:

– необходимо определить перечень средств вычислительной техники, в том числе портативных мобильных средств (ноутбуков, планшетов, мобильных устройств) которые будут предоставлены сотрудникам для удаленной работы;

– определить перечень информации и информационных ресурсов (программ, каталогов, файлов), расположенных в корпоративной информационной системе предприятия, к которым будет предоставляться удаленный доступ [5];

– исключить возможность установки работников иного программного обеспечения на устройство предоставленное предприятием;

– установить на рабочий компьютер все необходимые программно-аппаратные средства защиты, антивирус и другие программы для защиты информации;

– рекомендуется производить подключение к корпоративной информационной системе предприятия только по защищенным каналам связи по возможности с использованием технологий виртуальных частных сетей;

– обеспечить безопасную настройку рабочих компьютеров удаленных сотрудников для повышения защиты на уровне данных, приложений и операционной системы;

– назначить минимально необходимые права и привилегии для пользователей для осуществления своих трудовых функций;

– настроить политики безопасности на рабочих компьютерах;

– рекомендуется использовать по возможности многофакторную аутентификацию сотрудника при доступе к корпоративной информационной системе предприятия;

– при использовании электронного документооборота на предприятии желательно для каждого сотрудника, которые работают с юридически значимыми документами, оформить сертификат усиленной квалифицированной подписи;

– для более безопасного обмена документами следует завести для каждого удаленного сотрудника корпоративную рабочую почту [6].

– подготовить инструкции для сотрудников и администраторов информационной безопасности;

– провести инструктаж работников предприятия, осуществляющих удаленные доступ к корпоративным ресурсам, о правилах удаленного взаимодействия с данными компании;

– сотрудникам, отвечающим за обеспечение информационной безопасности необходимо осуществлять мониторинг деятельности и предотвращение возможных инцидентов;

– обеспечить своевременное блокирование удаленного сеанса доступа пользователя к корпоративной системе при выявлении подозрительной активности или при неактивности более установленного предприятием времени;

– обеспечит возможность оперативного реагирования администраторов информационной безопасности и принятия мер защиты информации при возникновении компьютерных инцидентов.

В конечном итоге у каждого сотрудника должно быть свое максимально защищенное удаленное рабочее место, при этом оно должно быть безопасно интегрировано в единую корпоративную информационную систему предприятия.

Если сотрудник использует личное устройство для удаленной работы, то на нем должен быть установлено антивирусное программное обеспечение для защиты от вредоносного кода или межсетевой экран, который позволяет повысить уровень информационной безопасности устройства.

При выполнении данных рекомендация невозможно полностью избавиться от рисков и угроз информационной безопасности, однако, возможно их минимизировать. Также необходимо учитывать тот факт, что основная роль в обеспечении защищенности корпоративных данных при удаленной работе 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.

Заключение. Удаленный доступ сотрудников к информационным системам предприятия может привести к утечке конфиденциальных данных и нарушению работы корпоративных систем вследствие неосторожности, как самих сотрудников, так и злонамеренных действий киберпреступников, поэтому требуется качественная настройка системы информационной безопасности и применения различных технологий и средств, способных контролировать работу сотрудников, чтобы максимально уменьшить риски утечки корпоративных данных [7].

Используя все вышеперечисленные рекомендации, возможно избежать большинство угроз, рисков и компьютерных инцидентов связанных с информационной безопасностью корпоративных данных предприятия. Минимизируя минусы удаленной работы, возможно будет сконцентрироваться только на достоинствах 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 прибыли.

Однако, даже не имея на своем предприятии высококвалифицированного персонала для настройки удаленного доступа к рабочим местам, любое предприятие способно существенно повысить информационную безопасность своих корпоративных данных и

понизить риски, связанные с удаленной работой, выполнив предложенные рекомендации, которые описаны в данной статье.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 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.

2. Носков С.И., Бутин А.А. Методическое обеспечение оценки уровня уязвимости объектов информатизации // Информационные технологии и математическое моделирование в управлении сложными системами. Иркутск: ИрГУПС. – 2015. – №14. – С. 38-48.

3. Малюк, А.А. Основы защиты информации: учебное пособие / А.А. Малюк. – М.:МИФИ, 2014. – 306 с.

4. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (с последними изменениями от 01.09.2021) Глава 49.1 «Особенности регулирования труда дистанционных работников» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 15.11.2021).

5. Письмо ФСТЭК России от 20.03.202 г. №240/84/389 «Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры» [Электронный ресурс]. – Режим доступа: http://www.fstec.ru (дата обращения: 15.11.2021).

6. Как обеспечить информбезопасность при переводе сотрудников на удаленную работу [Электронный ресурс]. – Режим доступа: https://www.reksoft.ru/blog/2020/04/10/office_home_protection/ (дата обращения: 15.11.2021).

7. Голосов, П.Е. «Оценка угроз информационной безопасности в условиях массового перехода на удаленную работу». – 2020. – 26 марта. – [Электронный ресурс]. – Режим доступа: https://udalenka.cdto.ranepa.ru (дата обращения 15.11.2021).

8. Россия сэкономит более 1 трлн рублей от перехода на дистанционную работу в 202 году // 1С-Битрикс. – [Электронный ресурс]. – Режим доступа: https://www.1c-bitrix.ru/about/news/1385822/ (дата обращения 15.11.2021).

REFERENCES

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

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

3. Malyuk, A.A. Fundamentals of information security: textbook / A.A. Malyuk. - M.: MEPhI, 2014. - 306 p.

4. Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ (with the latest amendments as of September 1, 2021) Chapter 49.1 "Features of labor regulation of remote workers" [Electronic resource]. - Access mode: http://www.consultant.ru (date of access: 15.11.2021).

5. Letter of the FSTEC of Russia dated 20.03.202, No. 240/84/389 "Recommendations for ensuring the security of critical information infrastructure facilities when implementing a remote mode of execution of official duties by employees of critical information infrastructure subjects" [Electronic resource]. - Access mode: http://www.fstec.ru (date of access: 15.11.2021).

6. How to ensure information security when transferring employees to remote work [Electronic resource]. - Access mode: https://www.reksoft.ru/blog/2020/04/10/office_home_protection/ (date of access: 15.11.2021).

7. Voices, P.E. "Assessment of information security threats in the context of a massive transition to remote work." - 2020 .- March 26. - [Electronic resource]. - Access mode: https://udalenka.cdto.ranepa.ru (date of treatment 11/15/2021).

8. Russia will save more than 1 trillion rubles from the transition to remote work in 202 // 1C-Bitrix. - [Electronic resource]. - Access mode: https://www.1c-bitrix.ru/about/news/1385822/ (date of treatment 11/15/2021).

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. Обеспечение информационной безопасности предприятия в условиях массового перевода сотрудников на удаленную работу [Электронный ресурс] // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журнал. – 2021. – №4(12). – С. 39-46 – DOI: 10.26731/2658-3704.2021.4(12).39-46 – Режим доступа: http://ismm-irgups.ru/toma/412-2021, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 27.01.2022)

For citation

Ass E.S., Butin A.A. Ensuring information security of an enterprise in the conditions of mass transfer of employees to remote work [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], 2021. No. 4(12). P. 39-46. DOI: 10.26731/2658-3704.2021.4(12).39-46 [Accessed 27/01/22]