**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ**

**«УНИВЕРСИТЕТ «ДУБНА»**

(государственный университет «Дубна»)

Кафедра системного анализа и управления

**ОТЧЕТ**

**по дисциплине (модулю)**

**«ПРОФЕССИОНАЛЬНАЯ ЭТИКА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»**

**Тема: «ПРИКЛАДНАЯ ЭТИКА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»**

**Выполнил**: студент гр. \_\_\_\_\_\_5013\_\_\_\_

\_\_\_\_\_\_\_\_ \_Попов С. Б.\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Руководитель:**

Минзов А. С.\_\_\_ \_\_\_\_\_\_\_\_ \_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Дубна 2019 г.**

Содержание

[Ситуация 1 3](#_Toc27795923)

[1.1 Профессиональная ситуация 3](#_Toc27795924)

[1.1.2 Описание ситуации 3](#_Toc27795925)

[1.1.3 Задача 3](#_Toc27795926)

[1.2 Оценка ситуации с точки зрения профессиональной этики 3](#_Toc27795927)

[1.3 Моделирование последствий решения об установке системы видеонаблюдения для сотрудников. 4](#_Toc27795928)

[1.4 Оценка возможности альтернативных решений 5](#_Toc27795929)

[1.5 Прогнозирование компенсирующих решений 6](#_Toc27795930)

[Ситуация 2 7](#_Toc27795931)

[2.1 Профессиональная ситуация 7](#_Toc27795932)

[2.1.2 Описание ситуации 7](#_Toc27795933)

[2.1.3 Задача 7](#_Toc27795934)

[2.2 Оценка ситуации с точки зрения профессиональной этики 7](#_Toc27795935)

[2.3 Моделирование последствий решения на установку скрытого наблюдения за сотрудником 8](#_Toc27795936)

[2.4 Оценка возможности существования альтернативных решений 9](#_Toc27795937)

[2.5 Прогнозирование компенсирующих решений 9](#_Toc27795938)

[Ситуация 3 10](#_Toc27795939)

[3.1 Профессиональная ситуация 10](#_Toc27795940)

[3.1.1 Описание ситуации 10](#_Toc27795941)

[3.1.2 Задача 10](#_Toc27795942)

[3.2 Оценка ситуации с точки зрения профессиональной этики 10](#_Toc27795943)

[3.3 Моделирование последствий решения на выявление предпочтений пользователей в ИНТЕРНЕТ путем изучения информации, передаваемой методами GET и POST 11](#_Toc27795944)

[3.4 Оценка возможности существования альтернативных решений 11](#_Toc27795945)

[3.5 Прогнозирование компенсирующих решений 12](#_Toc27795946)

[Список литературы 13](#_Toc27795947)

Ситуация 1

* 1. Профессиональная ситуация

В соответствии с заданием рассматривается ситуация №1: **Скрытое видеонаблюдение за сотрудниками.**

1.1.2 Описание ситуации

Как правило, наблюдение за работником ведется негласно, без его согласия. Позиция многих работодателей состоит в том, что в рабочее время работник обязан заниматься исключительно исполнением трудовых обязанностей. В качестве обоснования приводится ч. 1 ст. 91 ТК РФ[1], в которой определено, что «Рабочее время — время, в течение которого работник в соответствии с правилами внутреннего трудового распорядка и условиями трудового договора должен исполнять трудовые обязанности, а также иные периоды времени, которые в соответствии с настоящим Кодексом, другими федеральными законами и иными нормативными правовыми актами Российской Федерации относятся к рабочему времени…». Иными словами, предполагается, что на рабочем месте работник не имеет права на частную жизнь. В противном случае он недобросовестно использует то время, которое оплачивает работодатель, и совершает дисциплинарный проступок (неисполнение должностных обязанностей). Из этого делается вывод о том, что согласия работника на сбор информации о его поведении на рабочем месте не требуется. [2].

Также к целям установки видеонаблюдения относят:

* Организация безопасного рабочего пространства.
* Борьбу с недобросовестным выполнением работниками своих служебных обязанностей.
* Обеспечение пожарной безопасности.
* Неправомерное использование имущества работодателя в личных целях

С другой стороны, такое толкование данной нормы, ошибочно и нарушает права работника.

1.1.3 Задача

Таким образом, задачей данной работы является проведения анализа этичности внедрения и использования системы скрытого видеонаблюдения за сотрудниками.

* 1. Оценка ситуации с точки зрения профессиональной этики

Во-первых, этим нарушается конституционное право гражданина на неприкосновенность частной жизни [3], по­скольку сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не [4]. Европейский суд по правам человека неоднократно подчеркивал, что даже в публичной сфере существует зона взаимодействия человека с другими людьми, которая может относиться к сфере «частной жизни»

Во-вторых, если работник на рабочем месте в полном объеме выполняет нормы выработки и требования должностной инструкции по данной трудовой функции, то даже частные перекуры и личные разговоры по телефону не дают оснований работодателю наказывать работника за неисполнение трудовых обязанностей. Соответственно, теряется сам смысл в установлении слежения за работником в виду подобного аргумента.

В-третьих, работник имеет право на полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте [5], в т.ч. за способами контроля в отношении его производственной деятельности. Излишняя регламентация поведения работника на рабочем месте, не связанная с трудовыми обязанностями работника, а обусловленная лишь субъективным усмотрением работодателя, незаконна. Конечно, имеются профессии, которые предполагают полную концентрацию на производственном процессе — охранники, телохранители, авиадиспетчеры и т.п., но все же к большинству профессий таких жестких требований не предъявляется Моделирование последствий решения на установку скрытого видеонаблюдения за сотрудниками

* 1. Моделирование последствий решения об установке системы видеонаблюдения для сотрудников.

При размещение скрытого видеонаблюдения со стороны работодателя можно найти следующие плюсы:

* защита жизни и собственности от посягательств, сохранность личных вещей сотрудников и работодателей;
* создание доказательной базы для разрешения конфликтных ситуаций (помогает достичь истины при наличии разногласий между начальниками/подчиненными/коллегами/клиентами, пресекает «пустые» слухи о предосудительном поведении работников, подтверждает факт присутствия/отсутствия человека в указанной зоне и пр.) однако это раскроет факт скрытого слежения за сотрудниками, и данные доказательства будет не действительны в суде, так как добыты не законным путем ;
* контроль эффективности сотрудника (фиксация времени прихода и ухода, «перекуров», «обедов», анализ модели поведения на рабочем месте);
* повышение эффективности управления персоналом (знание психологии и умение анализировать поведенческие реакции поможет работодателю правильно оценить сотрудника и раскрыть его потенциал);

С другой стороны, это повлечет за собой и отрицательные моменты, такие как:

* нарушение этических норм и права человека на частную жизнь, видеокамеры фиксируют не только рабочие моменты, но и личное время в период перерывов, когда работник рассчитывает на отдых;
* создание нервной обстановки для сотрудников осознание постоянного скрытого наблюдения за каждым шагом плохо отражается на психоэмоциональном состоянии работников;
* отвлечение работодателя от основных обязанностей, некоторые руководители могут заразиться манией контроля, расходуя рабочее время на отслеживание перемещений своих подчиненных;
* формирование предвзятого отношения работодателя к сотруднику компании
* высокая стоимость в случае, если работник захочет начать судебное разбирательство в незаконной видеофиксации действий.
  1. Оценка возможности альтернативных решений

Возможная альтернатива, (легальная), это вести не скрытое видеонаблюдение.

Если работодателю необходим такой контроль за работниками, ему стоит установить камеры официально. В Правилах внутреннего распорядка нужно не просто указывать на наличие систем слежения, но и привести обоснование производственной необходимости в установке камер слежения. Кроме этого, в каждом рабочем помещении, где установлено видеооборудование, должна быть соответствующая табличка.

Доступ к персональным данным работников должны иметь только специально уполномоченные лица. При этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций. Кроме того, лица, получающие персональные данные работника, обязаны соблюдать режим секретности. Поэтому технические работники, ответственные за видеонаблюдение, в обязательном порядке должны быть ознакомлены с Положением о защите персональных данных.

Показ и распространение снятой в офисе видеокассеты также должны быть строго регламентированы. Например, видео­запись каких-либо виновных действий работника может быть просмотрена непосредственным начальником и руководителем организации, поскольку именно от них зависит вопрос о наложении взыскания.

* 1. Прогнозирование компенсирующих решений

При легальном размещении камер видео наблюдений, у сотрудника будет меньше психологических триггеров, что поможет ему более спокойно относиться к слежению за ним, так как у него паронайноного чувства «а вдруг за мной следят», он будет точно знать, что следят и в скором времени привыкнет. Так же он будет знать, в каких местах он может насладится частной жизнью, например «курилка» и знать, что у него есть уголок безопасности.

Таким образом, организация видеонаблюдения в офисе или производственном помещении требует соблюдения многих условий. В противном случае работодатель может оказаться в различных неприятных ситуациях — от потери лояльности сотрудников, узнавших о системе слежения по слухам, до проигрыша дела в суде.

Ситуация 2

2.1 Профессиональная ситуация

В соответствии с заданием рассматривается ситуация №2: **Скрытое наблюдение за сотрудником.**

2.1.2 Описание ситуации

По данным различных исследований, проведенных в последние 5 лет, до 80% компаний в той или иной степени ведут слежку за своими работниками. Из них 40-60% мониторят рабочие компьютеры сотрудников, 30% ограничиваются видеокамерами и системами контроля доступа, до 30% используют широкий комплекс технических средств для мониторинга.

контролировать персонал нужно — в конце концов, это одна из важнейших функций менеджмента. Научно доказано, что разумный контроль дисциплинирует сотрудников, повышает продуктивность и предупреждает “инсайдерские” угрозы. Нет ничего плохого в камерах видеонаблюдения в офисе и даже в так называемых СКУДах, контролирующих приходы-уходы. Лояльные работники вполне понимают, что в некоторых случаях необходимо фиксировать, сколько времени кто отработал за компьютером и какие сайты посещал — без такого софта не обойтись, к примеру, если в вашем штате трудятся “удаленщики”.

Однако зачастую работодатели, все же могут зайти немного дальше. [6]

* + 1. Задача

Таким образом, задачей данной работы является проведения анализа этичности внедрения и использования системы скрытого наблюдения за сотрудником.

* 1. Оценка ситуации с точки зрения профессиональной этики

Статья 23 Конституции РФ [3] говорит, что каждый человек имеет право на неприкосновенность личной жизни и тайну переписки. Ей едва не противоречит статья 22 Трудового кодекса РФ [7] о том, что «работодатель может требовать от работников исполнения ими трудовых обязанностей» и «соблюдения правил внутреннего трудового распорядка».

То есть по ТК компания имеет право на контроль подчиненных, в том числе с помощью специальных программ. Если работодатель отслеживает трафик, проверяет историю браузера и корпоративную почту — это законно.

Соцсети, мессенджеры и некорпоративная почта относятся к личной переписке. По идее, ни работодатель, ни любой другой человек не имеют права их проверять. Но если сотрудник переписывается в мессенджерах на работе, все не так однозначно.

Работодатель купил время сотрудника, и любой факт личной переписки противоречит условиям трудового контракта, так что в рабочее время переписка перестает быть личной [8]. Использование программ контроля за сотрудниками не противоречит указанным нормам. Более того, дополнительной гарантией взаимопонимания для сторон может стать заключение договора, в котором будет указано о необходимости использования подобных программ. В таком случае со стороны работодателя не будет умысла нарушать права сотрудника.

В случае если такого договора нет, то работодатель нарушает следующие законы:

* Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
* Нарушение неприкосновенности частной жизни
* Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Что является не этичным.

* 1. Моделирование последствий решения на установку скрытого наблюдения за сотрудником

Скрытое незаконное наблюдение тоже принесет пользу, работодателю:

* Поможет найти человека, который занимается не законным распространением коммерческой тайны
* Человека, который впустую просиживает, и за пользование соц. сетями зарабатывает деньги

Некоторые организации выбирают для слежки за подчиненными по-настоящему шпионское ПО. Как правило, такие приложения работают в фоновом режиме на рабочих ПК и даже на мобильных устройствах, совершенно незаметно для пользователя. Другими словами, работодатель может поставить свой шпионский софт на каждый рабочий смартфон, передать их своей команде и затем во всех подробностях отслеживать, как люди работают.

GPS-контроль. Эту технологию слежки за сотрудниками удобно использовать в рабочие часы, особенно для таких бизнесов, как службы доставки или агентства недвижимости. В шпионских приложениях GPS-трекинг функционирует так, что человек и не подозревает, когда за ним следят, в это время он может нам солгать и мы можем выявить потенциально слабое звено в организации.

Для коммерческих структур также существует разного рода информация, которую лучше не разглашать. она позволит поставить под угрозу существование одного конкретного предприятия.

* 1. Оценка возможности существования альтернативных решений

Всё начинается с того, что, работодатель должен быть открыт перед своими работниками и сразу оповестить их, о наличии официального слежения за ними. Тогда работник сам будет понимать, что:

Во-первых, нужно разграничивать личную информацию и служебную, на рабочем месте человек обязан обрабатывать и работать со служебной информацией, которую работодатель вправе контролировать. На рабочем месте, сотрудник обязан использовать ПК как рабочий инструмент и обрабатывать служебную информацию.

Придя на работу, сотрудник, не располагает своим временем, это время он продал работодателю, таким образом, получается, что человек, тратящий рабочее время на личные нужды, априори нарушил трудовой договор, не говоря уже о морально-этической стороне.

Второй важный момент — прозрачность их использования. Сотрудник будет работать с большей отдачей, зная, какие именно функции программы контроля активированы, какая информация может собираться и т.д. Одно лишь понимание этого будет мотивацией для использования рабочего времени в рабочих же целях.

2.5 Прогнозирование компенсирующих решений

Сотрудник должен понимать, что, придя на работу, он будет обязан сосредоточиться на ее выполнении. При этом он четко знает формы и методы контроля и сюрпризов для него не предвидится. Кроме того, ответственность за явные нарушения прав четко предусмотрена действующим законодательством. В конечном итоге, это вопрос личного выбора человека: вида деятельности, формата работы, компании, в конце концов.

Таким образом, при юридически грамотном подходе, проблемы в использовании таких программ нет. Просто нужно уметь находить правильные решения и закреплять их во взаимовыгодных соглашениях. Сотрудник и работодатель не должны находиться по разные стороны баррикад, а понимать, что делают общее дело и уважать права и ответственность друг друга, четко выполняя взаимные обязанности [9].

Ситуация 3

3.1 Профессиональная ситуация

В соответствии с заданием рассматривается ситуация №50: **Скрытое выявление предпочтений пользователей в ИНТЕРНЕТ путем изучения информации, передаваемой методами GET и POST.**

3.1.1 Описание ситуации

С Современные веб-ресурсы не просто предоставляют информацию посетителю, но и взаимодействуют с ним. Для взаимодействия с пользователем нужно получать некоторую информацию от него. Для получения данных есть несколько методов, очень распространенные методы GET и POST. И соответственно в PHP есть поддержка этих методов передачи данных GET и POST. Посмотрим, как работают эти методы.

Данный метод передачи переменных применяется в PHP для передачи переменных в файл при помощи адресной строки. То есть переменные передаются сразу через адресную строку браузера.

Передача данных методом POST позволяет скрыто передавать переменные с одного файла в другой. Однако существуют средства перехвата таких запросов из браузера.

* + 1. Задача

Провести анализ этичности скрытого выявления предпочтений пользователей ИНТЕРЕНЕТ путем изучения информации, передаваемой методами GET и POST.

* 1. Оценка ситуации с точки зрения профессиональной этики

Перехват трафика может быть частью не честно работающего интернет ресурса, для того чтобы более правильно предлагать контекстную рекламу. Большинство браузеров и поисковых ресурсов собирает информацию из наших запросов чтобы предлагать более релевантные предложения. Так же таким образом интернет гиганты зарабатывают с помощью нас, продавая информацию о наших запросах в интернет-магазинах, в следствии чего мы видим навязчивую рекламу. С одной стороны, пользователь подтверждает просмотр запросов браузером, когда устанавливает браузер. Большинство браузеров позволяет отключить, анализ исходящего трафика.

Но это не все проблемы, за частую Get и POST запросы обрабатываются хакерами.

Хакеры могут получать доступ к исходящим запросам с помощью **снифферов**.

Снифферы — это программы, способные перехватывать и впоследствии проводить анализ сетевого трафика. Снифферы полезны в тех случаях, когда нужно перехватить пароли или провести диагностику сети. Программу можно установить на одном устройстве, к которому есть доступ и в течение короткого времени получить все передаваемые данные из подсети [10].

3.3 Моделирование последствий решения на выявление предпочтений пользователей в ИНТЕРНЕТ путем изучения информации, передаваемой методами GET и POST

С помощью перехвата трафика сниффером, злоумышленник может:

* Перенаправлять наш сетевой трафик с помощью изменения пакета и отправить нас на другой сетевой ресурс, в своих целях
* Если у вас есть доступ к закрытому ресурсу, злоумышленник может узнать каким запросом вы Post или Get запросом вы получаете доступ к сайту, и может получить доступ к этим данным ведь он знает каким, запросом они достаются
* Не редкостью является и перехват логинов и паролей с помощью изучения get post запросов, так как многие сайты, используют именно эти запросы для передачи авторотационных запросов
* Так же хакеры в процессе изучение запросов, получить доступ к личной информации жертвы
* Не редко жертвами хакеров могут стать не пользователи, а интернет ресурсы.

Изучение поисковых запросов для владельца сайта, Get и Post запросы служат предметом выдачи более подходящей рекламы

3.4 Оценка возможности существования альтернативных решений

Сайты, собирающие информацию, могут провести опрос пользователя, на тему того какую рекламу он хочет видеть, в таком случае можно не анализировать запросы.

Для владельцев сайтов, изобретать более изощренные способы передачи и защиты информации, для того чтобы было сложнее анализировать трафик.

Для пользователя, нужно быть очень внимательным, устанавливать антивирусы лицензионные антивирусы, которые смогут анализировать трафик, который вернулся на запрос и в случае возникновения подозрения от ресурса, оповестят вас и предложат пути решения проблемы.

3.5 Прогнозирование компенсирующих решений

Для получения информации от пользователя для сайтов и интернет-магазинов, лучше напрямую спросить у пользователя, что ему хотелось бы видеть в качестве рекламы.

Для защиты от хакеров нужно быть очень внимательным, ведь из за ошибки можно не только потерять логин и пароль от сайта, возможно вы там оставили еще какую ценную информацию, которой хакеры, смогут воспользоваться, тогда и масштаб проблемы будет серьезнее.

Список литературы

1. <http://www.consultant.ru/document/cons_doc_LAW_34683/bd14cccf0a1f074ef104e82522f7e2dea04d651f/vo>
2. <http://www.delo-press.ru/articles.php?n=6772>
3. <https://ppt.ru/kodeks.phtml?kodeks=0&paper=23>
4. <https://ppt.ru/kodeks.phtml?kodeks=0&paper=24>
5. <http://www.consultant.ru/document/cons_doc_LAW_34683/faedf3a7c3cd35871542ce0c323e898871ca1753/>
6. <https://ideanomics.ru/articles/17328>
7. [https://ppt.ru/kodeks.phtml?kodeks=0&paper=2](https://ppt.ru/kodeks.phtml?kodeks=0&paper=24)2
8. <https://b2blog.beeline.ru/kak-zakonno-sledit-za-sotrudnikami/>
9. <https://habr.com/ru/company/atompark_software/blog/133618/>
10. <https://www.anti-malware.ru/threats/sniffers>