Юридические аспекты внедрения приложений мониторинга деятельности офисных сотрудников на рабочих местах

17 апреля 2020 г., Москва

Юрий Основский
Руководитель группы технической поддержки (московское отделение)
ООО «Атом Безопасность»

ООО Атом Безопасность

— 10 лет разработки приложений контроля сотрудников
— Академгородок Новосибирск, резиденты Технопарка
— Высокотехнологичная компания с опытной командой разработчиков-профессионалов в области ИБ

Программные комплексы ИБ

- DLP-системы (Data Leak Prevention) – программные комплексы предотвращения утечки данных, служат, как понятно из названия, предотвращения утечек (намеренных или непреднамеренных), могут перенаправлять информационные потоки. Одна из наиболее известных систем - DeviceLock;
- Программные комплексы мониторинга работы пользователей – комплексы для сбора и анализа событий работы пользователей: запуска приложений, редактирования документов, посещений сайтов, печати документов. Наиболее известные системы – StaffCop Enterprise, «Стахановец», SearchInform, в них есть элементы DLP;
- SIEM-системы (Security Information and Event Management) – мощные системы анализа в реальном времени событий информационной безопасности, исходящих от сетевых устройств и приложений. SIEM могут быть приложениями, устройствами или даже услугами. Применяются также для журналирования данных, операций с ними и генерации отчётов. Очень часто данные, собранные первыми двумя группами, передаются в SIEM-системы.

Что гласит Законодательство?

С одной стороны:

Конституция РФ, Статья 23:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Уголовный кодекс РФ, Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений:

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом …, либо обязательными работами …, либо исправительными работами

Что гласит законодательство?

С другой стороны:

Гражданский кодекс, Статья 1470. Служебный секрет производства:

1. Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю.

Статья 15 Трудового кодекса РФ:

"Трудовые отношения - отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции (работы по определённой специальности, квалификации или должности), подчинении работника правилам внутреннего трудового распорядка при обеспечении работодателем условий труда, предусмотренных трудовым законодательством, коллективным договором, соглашениями, трудовым договором.

Разграничение личной и служебной информации

На рабочем месте:

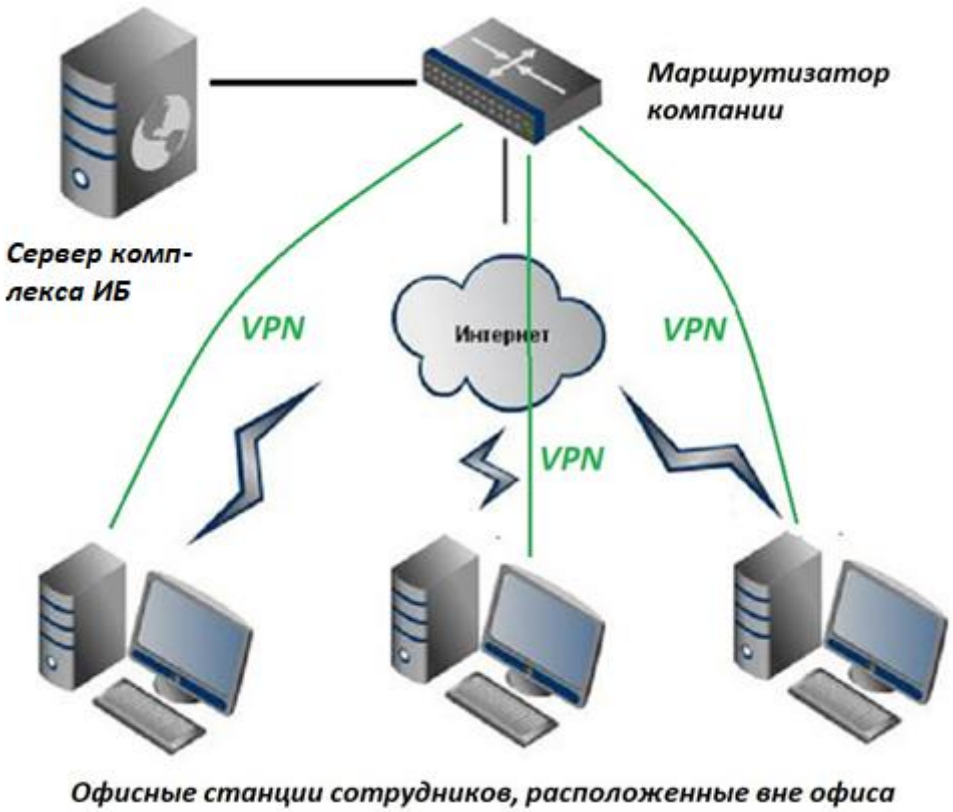
- Компьютер и телефон – для выполнения должностных обязанностей, а не для личных целей
- Владелец электронного почтового ящика, абонент телефонной сети – организация, а не физическое лицо
- Работник ведёт не личную переписку, а выполняет трудовые обязанности и указания работодателя;
- Весь бумажный документооборот ведётся через специализированные отделы (канцелярии, секретариаты), фактически с тотальным контролем переписки.

Должны быть приняты соответствующие регламенты и правила, которые утверждаются приказом руководства предприятия.

Обязательные действия перед началом внедрения системы мониторинга

- Определить и довести до работников правила использования средств хранения, обработки и передачи информации
- Разработать и довести до работников регламент проведения мониторинга
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору или корректировка коллективного договора)

Использование оборудования на «удалёнке»: вариант 1 - офисное

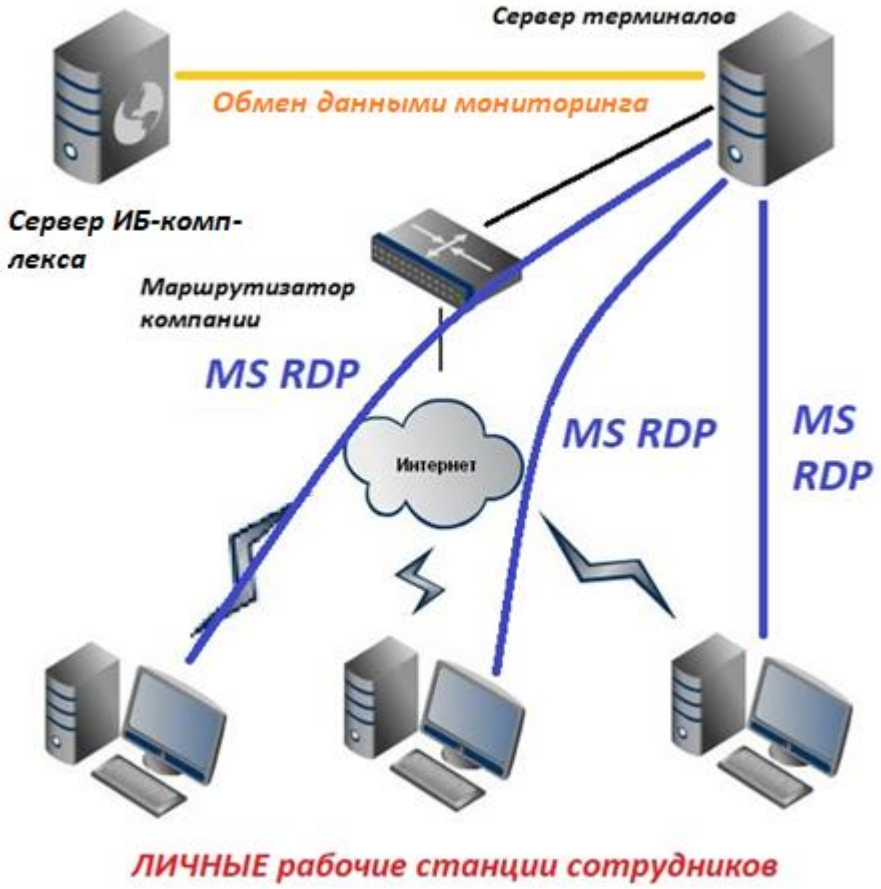


Офисные станции сотрудников, расположенные вне офиса

Оборудование, принадлежащее работодателю, передаётся сотруднику во временное пользование. Сотрудники работают в привычных им средах, используя те же программы и оборудование, что и при офисной работе.

В этом случае необходимо оформить передачу оборудования сотруднику на ответственное хранение и использование, причём аппаратная конфигурация офисной рабочей станции (с серийными номерами оборудования), как и перечень установленного ПО, должны быть указаны в Акте приёма-передачи, чтобы исключить злоупотребления со стороны нечестных сотрудников.

Использование оборудования на «удалённке»: вариант 2 – сервер терминалов



Сотрудники работают на своих ЛИЧНЫХ домашних компьютерах, офисные рабочие станции остались в офисе и выключены, чтобы с личных домашних компьютеров к ним доступа не было.

В этом случае без письменного согласия сотрудника средства мониторинга (или DLP-система) может быть установлена только на сервер терминалов.
Установка любого программного обеспечения для мониторинга на личную (домашнюю) рабочую станцию сотрудника может проводиться только с его письменного согласия, так как в этом случае в собираемую информацию может попасть личная информация сотрудника, что без его согласия недопустимо.

Использование оборудования на «удалёнке»: вариант 3 – только личные компьютеры сотрудников

Сотрудники работают на своих ЛИЧНЫХ домашних компьютерах, офисные рабочие станции остались в офисе и выключены, чтобы с личных домашних компьютеров к ним доступа не было.

Связи с офисом нет вообще никакой, обмен информацией идёт только по электронной почте.

В этом случае установка любого программного обеспечения для мониторинга на личную (домашнюю) рабочую станцию сотрудника может проводиться только с его письменного согласия, так как в этом случае в собираемую информацию может попасть личная информация сотрудника, что без его согласия недопустимо.

Особенности работы сотрудников отделов ИБ

Сотрудникам отдела ИБ необходимо убедиться, что офисные рабочие станции, передаваемые сотрудникам, не содержат на жёстких дисках информацию, подпадающую под регламенты коммерческой тайны и конфиденциальной информации (включая персональные данные сотрудников). Если такие данные будут обнаружены на жёстких дисках – их надо удалить.

Рекомендуется заключить дополнительные соглашения с сотрудниками отдела ИБ о неразглашении ставшей им случайно известной личной информации сотрудников.

Спасибо за внимание!

РАБОТАЙТЕ БЕЗОПАСНО!

Юрий Основский
Руководитель группы технической поддержки (московское отделение) ООО «Атом Безопасность»


+7 (499) 638-28-09 доб. 237
+7 (999) 347-86-77


y.osnovskiy@staffcop.ru