DOI https://doi.org/10.46845/2541-8254-2023-3(40)-53-53
УДК 004.42

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ УДАЛЕННОЙ РАБОТЫ СОТРУДНИКОВ ОРГАНИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Е. Головченко, специалист по защите информации
e-mail: dremartstud@gmail.com

ФГБОУ ВО «Калининградский государственный технический университет»

В статье были изучены и рассмотрены актуальные системы контроля удаленной работы для выявления минимального необходимого набора функционала для разработки подобной системы. Разработана система контроля удаленной работы для учета рабочего времени, сбора данных об открытых процессах, сетевой активности и распределения ресурсов рабочего компьютера, которая создает временную линию работы сотрудника (время, проведенное в определенном окне, и сколько раз оно было открыто). Приведенный набор функционала призван повысить уровень информационной безопасности организации.

Ключевые слова: *разработка системы контроля удаленной работы, удаленные сотрудники, повышение уровня информационной безопасности удаленной работы, система контроля удаленной работы*

ВВЕДЕНИЕ

В современном мире сложилась ситуация, в которой организации широко внедрили в структуру своего рабочего процесса протокол удаленной работы, что сделало проблемы, связанные с обеспечением информационной безопасности в таковых условиях, актуальными. Для организации самым дешевым, простым и эффективным методом перевода сотрудника на удаленную работу является использование личного устройства сотрудника, поскольку в данном случае будет задействован минимум финансовых средств и усилий со стороны организации. Однако данный метод содержит в себе определенное количество рисков и угроз информационной безопасности.

Безопасность – это защищенность от угрожающих факторов, защищенность от опасности. Также безопасность – это защищенность от гипотетического ущерба, который будет нанесен при реализации предполагаемых угроз [1].

Перевод сотрудников на удаленную работу повлек за собой множество новых уязвимостей и точек входа в корпоративные сети для злоумышленников, так как средства для защиты и контроля у многих компаний изначально не были внедрены [2]. Внедрение средств защиты, направленных на противодействие внутренним нарушениям, таких как DLP-системы, системы для контроля доступа, системы поведенческого анализа и прочие, необходимо и оказывает эффективное влияние по снижению инцидентов безопасности и утечек данных, а также заражения корпоративных сетей вредоносным программным обеспечением. Перевод на удаленную работу без внедрения систем контроля за дистанционными сотрудниками повлечет за собой рост умышленных нарушений и кражи информации, так как выявить утечку в таких условиях практически невозможно. Из данного следует, что при переводе на удаленную работу необходимо внедрить и настроить системы слежения за сотрудниками.

Программы учета рабочего времени и мониторинга продуктивности сотрудников позволяют получать аналитические данные об их поведении, что дает полное представление о производительности сотрудников за рабочими компьютерами. Это помогает выявлять

определенные закономерности продуктивной работы и наименьшей вовлеченности сотрудников и в соответствии с ними оптимизировать процессы. Анализ производительности сотрудников является важным инструментом регулирования полезного действия внутри организации, призванного снизить убытки и угрозы информационной безопасности.

ОБЪЕКТЫ ИССЛЕДОВАНИЯ

В роли объектов исследования выступают три системы контроля удаленной работы сотрудников: StaffCop, KickIdler, TopTracker. Проведен сравнительный анализ систем контроля удаленной работы сотрудников.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Целью данной работы является изучение систем контроля удаленной работы сотрудников и разработка системы контроля удаленной работы сотрудников для повышения уровня защищенности информационной системы.

Задачи работы: изучить системы контроля удаленной работы сотрудников и провести их сравнительный анализ; разработать механизм сбора информации об удаленной работе и всех процессах, происходящих на компьютере сотрудника.

МЕТОДЫ ИССЛЕДОВАНИЯ

В процессе исследования были использованы такие методы, как анализ научных работ, изучение профессиональной литературы, сравнение аналогичных программных решений и моделирование.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Разработанная система контроля удаленной работы для учета рабочего времени, сбора данных об открытых процессах, сетевой активности и распределения ресурсов рабочего компьютера создает временную линию работы сотрудника (время, проведенное в определенном окне, и сколько раз оно было открыто).

По данным опроса IT-сервиса по поиску работы и подбору сотрудников Superjob, всего о наличии удаленных сотрудников сообщили 51 % опрошенных компаний, у которых в четырех из десяти компаний дистанционно работает более 30 % персонала [3], что служит доказательством необходимости введения систем контроля удаленной работы.

Согласно статье трудового кодекса Российской Федерации «Особенности регулирования труда дистанционных работников», при заключении трудового договора можно предусмотреть обязанность использования работником предоставленных или рекомендованных работодателем программно-технических средств, оборудования, а также средств защиты информации и иных средств [4].

С 1 марта 2022 года законодателем прямо закреплено право работодателя в целях контроля за безопасностью производства работ использовать приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, обеспечивать хранение полученной информации [5]. Основополагающим документом при внедрении в систему организации является приказ об информационной безопасности, применении в организации технологии по контролю за качеством и количеством выполняемой работы, предотвращением утечек конфиденциальной информации.

Выполнять трудовую функцию в рабочее время – это обязанность работника, определенная трудовым договором, при этом он должен соблюдать правила внутреннего трудового распорядка организации и условия иных ЛНА работодателя [6].

Таблица 1 – Сравнительная характеристика программ учета рабочего времени и мониторинга работы: StaffCop [7], KickIdler [8] и TopTracker [9]

Staffcop	**Достоинства**	Просмотр неограниченного количества компьютеров. Запись видео с экранов. Совместимость с последними версиями Windows, Linux и MacOS. Простая установка. Функционал, позволяющий установить программу как в открытом режиме, так и в скрытом. Бесплатная версия программы с ограничением до шести пользователей
	Недостатки	Запись с экранов занимает много места на сервере. Цена. Ценообразование зависит от срока лицензии. Так, месячный тариф на одного сотрудника выходит дороже тарифа на три месяца. Если контроль необходим на больший срок, то целесообразна бессрочная лицензия
Kickidler	**Достоинства**	Сбор данных об активности сотрудников, их анализ, выявление возникающих проблем и решение их в нужное время. Автоматический и статистический анализ данных, цель которого – оперативное выявление подозрительной активности пользователей. Выявляются инциденты, нелояльные сотрудники и инсайдеры. Автоматические оповещения, о нарушениях сотрудниками политики безопасности или любых других действиях, которые непродуктивны или опасны. Конструктор отчетов – интерфейс отображения информации, который призван предварительно настроить отчеты. Блокировка нежелательной активности. Если есть возможность – запретите сотрудникам посещать определенные веб-сайты, запускать определенные приложения и использовать съемные USB-накопители, что снизит риск заражения компьютеров на рабочих местах и локальной сети компании вредоносными программами и повысит производительность сотрудников
	Недостатки	Датированная многоступенчатая настройка сервера и клиента по модели распространения по подписке. Нет облачного интерфейса администратора
Toptracker	**Достоинства**	Бесплатная программа учета рабочего времени без необходимости установки и настройки сервера. Совместимость с последними версиями Windows, Linux и MacOS. Присутствует веб-версия программы. Учет рабочего времени и полная статистика по работе на проекте. Не нарушает границы личной жизни сотрудников вне рабочего времени
	Недостатки	Небольшой набор функций программы. Не записывает посещенные сайты. Разработан зарубежной компанией

Исходя из представленной в таблице 1 информации можно сделать вывод о том, что программные комплексы для мониторинга удаленной работы сотрудников имеют обширный функционал, включающий в себя ограниченные по возможности DLP-системы, SIEM-системы и системы поведенческого анализа. Программный комплекс Kickidler включает в себя наибольший набор функций, нежели рассмотренные аналоги. Однако данный функционал, возможно, понадобится не всем организациям, так как у них уже могут быть внедрены свои решения либо нет необходимости в таких программных комплексах. Также не все организации

имеют возможность выделить бюджет на внедрение таких дорогих программ в свою рабочую среду. В таблице 2 приведены расчеты стоимости лицензий Kickidler и Staffcop на разные периоды времени.

Таблица 2 – Сравнение стоимости лицензий для организации с 40 сотрудниками KickIdler [10], StaffCop [11] и TopTracker

Период действия лицензии	**Стоимость 40 лицензий Kickidler**	**Стоимость 40 лицензий Staffcop**	**Стоимость 40 лицензий TopTracker**
1 месяц	24 000 ₽	нет	Бесплатно
3 месяца	60 000 ₽	40 680 ₽	
6 месяцев	104 000 ₽	81360 ₽	
1 год	158 400 ₽	126 000 ₽	
3 года	316 800 ₽	327600 ₽	

В сравнении с платными аналогичными программными комплексами слежения за работой сотрудников и учета их рабочего времени бесплатное решение, которое предоставляет лишь систему учета рабочего времени, не позволяющую выгружать данные о компьютере, открытых окнах, запущенных процессах и так далее в другие программы, можно считать ограниченным и неполноценным. Если у организации имеются оплаченные лицензии и внедрены SIEM, DLP или UEBA-системы, достаточно собрать данные об активности сотрудника, представить их в необходимом формате и передать системам анализа, что значительно снизит расходы организации.

Таким образом, создание бесплатной системы, позволяющей как следить за работой сотрудников и учитывать рабочее время сотрудников, так и вести учет открытых процессов, временной линии посещенных программ и окон внутри системы, создавать слепок из системы для выявления потенциальной угрозы информационной безопасности рабочей станции, которая затем организует в необходимом виде все данные и выгрузит их в JSON формате, – является актуальным и необходимым.

Данные из JSON можно при помощи любого языка программирования представить в виде диаграмм, графиков, проанализировать их и сделать выводы о безопасности используемого компьютера.

В системе регистрируются все происходящие события, которые имеют отношение к информационной безопасности, следовательно должен использоваться механизм аудита. Аудит обеспечивает анализ последствий нарушения информационной безопасности и способствует выявлению злоумышленников. Такой аудит можно назвать пассивным [12].

В рамках данной работы была разработана консольная программа, представляющая из себя прототип комплекса для слежения, включающую в себя минимальный необходимый набор функций для слежения за удаленной работой сотрудников.

На рисунке 1 представлен алгоритм работы программы.

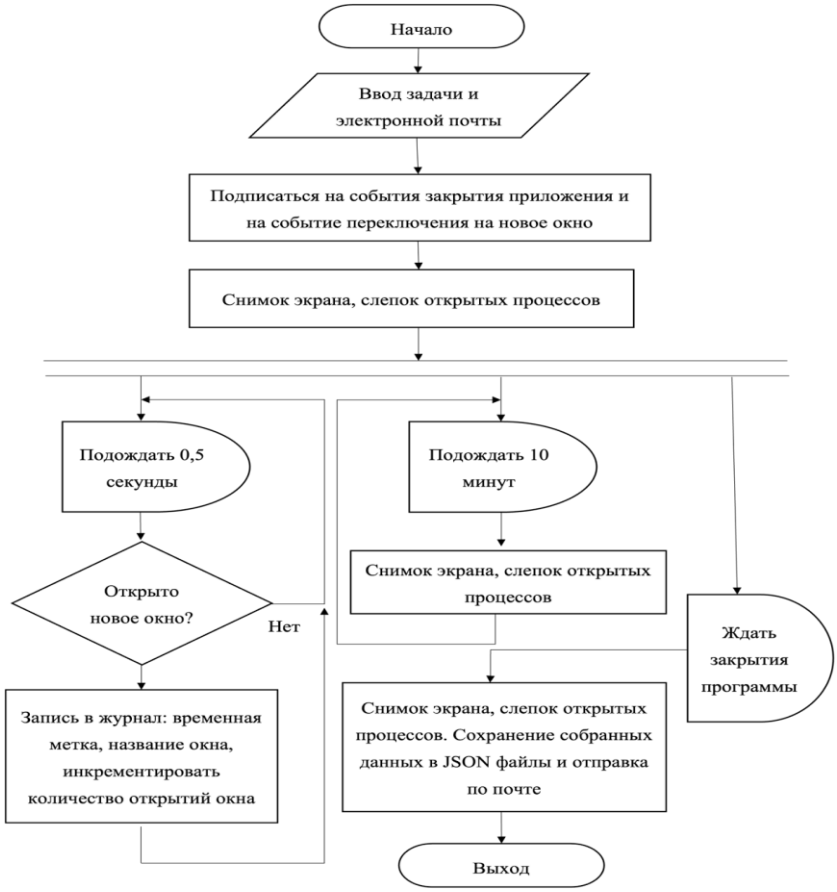

Рисунок 1 – Блок схема программы

При открытии программа запросит ввести название задачи, над которой будет вестись работа, и электронную почту, куда будут отосланы данные о работе сотрудника (рисунок 2).

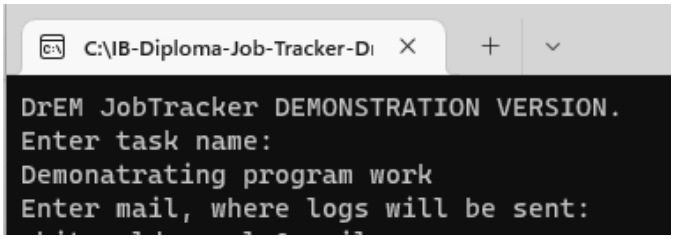

Рисунок 2 – Начало работы программы слежения за работой сотрудников

После того как пользователь ввел запрошенные программой данные, начинается учет его рабочего времени, запись отрытых окон, запись информации о посещенных окнах, открытых процессах и задействованных ресурсах рабочего компьютера (рисунок 3).

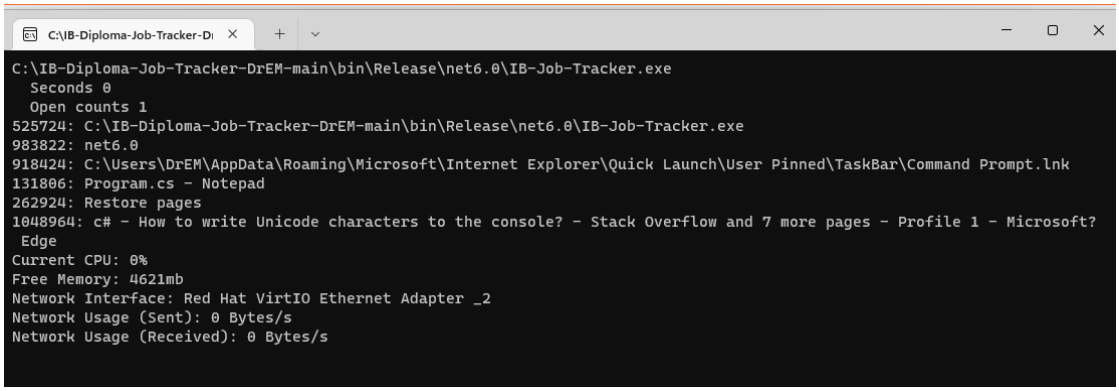

Рисунок 3 – Отображение открытых и записанных процессов

Разработанный программный комплекс слежения за работой сотрудника учитывает все открытые окна во время работы, сколько секунд они были открыты и сколько раз открывались.

На рисунке 4 изображены: название задачи; время начала работы; время прекращения работы; суммарное время работы; информация об открытых окнах (название окна, сколько раз оно было открыто, сколько секунд в нем было проведено).

Рисунок 4 – Отформатированный JSON, данные о проекте и об открытых окнах

Программа слежения за работой сотрудника способна определить любые открытые окна, включая вкладки в браузере, и все зафиксирует в общий массив данных. Также данная программа фиксирует временные метки, когда были открыты окна во время учета рабочего времени. Эти данные представлены на рисунке 5 в виде массива из двух полей – названия окна и временной метки, что представляет из себя данные для создания временной линии работы сотрудника.

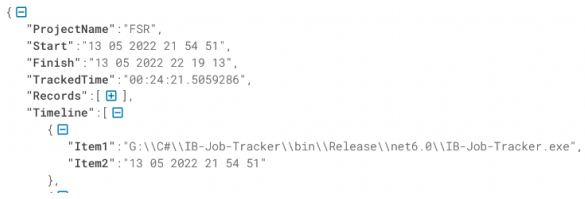

Рисунок 5 – Временная линия

Каждый заданный период времени программа сохраняет данные обо всех открытых процессах в системе, ресурсах системы и сетевой активности подключенных сетевых адаптеров (название сетевого адаптера, сколько бит отправлено и получено).

На рисунке 6 данные представлены в следующем виде: сколько свободно оперативной памяти, на сколько процентов загружен центральный процессор, какие сетевые адаптеры подключены к системе и сколько бит они отправили и получили.

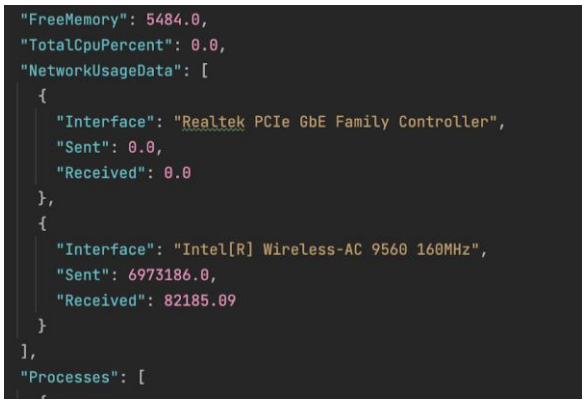

Рисунок 6 – Данные о ресурсах системы и открытых процессах

Помимо открытых процессов, программа фиксирует и сохраняет данные обо всех открытых окнах в системе (рисунок 7).

Рисунок 7 – Открытые окна в системе

Все данные и снимки экранов сохраняют в специальную папку с названием задачи в корне программы (рисунок 8).

Рисунок 8 – Папка с записанными данными

При подключении к сети Интернет программа отправит все записанные данные и снимки экрана на почту работодателя. Данное решение в будущем при дальнейшей разработке необходимо заменить на отправку по зашифрованным каналам на выделенный сервер в организации.

На рисунке 9 представлено письмо с информацией о работе сотрудника.

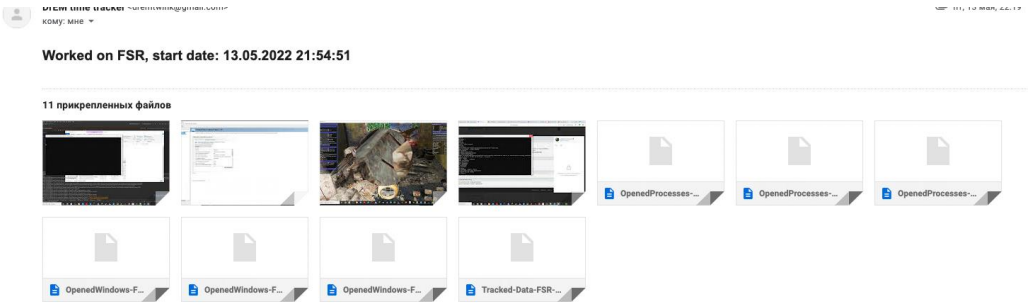

Рисунок 9 – Письмо с данными о работе сотрудника

При дальнейшей доработке и разработке данную программу можно представить на рынке программ слежения за удаленной работой сотрудников, написав дополнительное программное обеспечение для анализа работы сотрудников, что превратит программу в комплекс программ для обеспечения информационной безопасности удаленной работы.

ЗАКЛЮЧЕНИЕ

Разработано программное обеспечение для слежения за удаленной работой сотрудников. Работа программы не нагружает систему сотрудника, что позволяет не снижать его продуктивность. Сбор данных ведется исключительно во время работы. Весь код программы был написан на языке C# на платформе «.NET». При написании была использована документация по C# от компании Microsoft [13].

Главным преимуществом указанного программного обеспечения является бесплатный клиент для сбора данных об активных процессах и окон на компьютере работника, учета его рабочего времени и сохранение всех данных в формате JSON, а также возможность информирования о работе сотрудников по электронной почте.

Текстовый формат представления данных JSON является универсальным. Благодаря данному формату любой разработчик может написать короткий класс для интеграции данных в любую программу и производить любые необходимые манипуляции с ними. Также существуют бесплатные программы для автоматического представления данных формата JSON в код на необходимом языке программирования.

Все данные о работе сотрудника, о его системе и возможных злонамеренных процессах в диспетчере задач будут обработаны на удаленном компьютере работодателя, что минимизирует нагрузку на рабочий компьютер удаленного работника, не снижая продуктивность его работы.

Возможность получения администратором безопасности данных о любом удаленном рабочем компьютере в рабочее время позволит совершить сканирование безопасности устройств в организации без замедления работоспособности сотрудников, определить легитимность удаленного компьютера, а также отреагировать на выявленные угрозы и вредоносные процессы, что позволит минимизировать ущерб удаленной работы.

Были изучены и проанализированы системы контроля удаленной работы сотрудников, разработана система контроля удаленной работы сотрудников. Разработанная программа включает в себя следующий функционал: учет задачи, над которой ведется работа; уведомление о работе сотрудника по почте; периодический снимок активного экрана в заданном интервале времени; периодическая запись информации об открытых процессах в системе в заданном интервале времени; периодическая запись информации об открытых портах и сетевой деятельности устройства; периодическая запись информации о свободной оперативной памяти и ресурсах процессора и видеокарты; учет рабочего времени; учет того, над какой задачей ведется работа; создание временной линии посещенных окон; создание отчетов в формате JSON для интеграции в любые внедренные в организацию сервисы.

Цели, представляющие из себя изучение систем контроля удаленной работы сотрудников и разработку системы контроля удаленной работы сотрудников, были достигнуты.

Задача работы – разработка механизма сбора информации об удаленной работе и всех процессах, происходящих на компьютере сотрудника, была выполнена.

СПИСОК ЛИТЕРАТУРЫ

1. Бондарев,В. В. Введение в информационную безопасность автоматизированных систем : Учебное пособие / В. В. Бондарев. – Москва : Издательство МГТУ им. Н. Э. Баумана. 2016. – 250 с.
2. Гурова, И. М. Дистанционная работа как тренд времени: результаты массового опыта / И. М. Гурова // МИР (Модернизация. Инновации. Развитие). 2020. – Т. 11. – № 2. – С. 128–147.
3. Эксперты зафиксировали самый высокий уровень удаленки с мая 2020 года [Электронный ресурс]. – 2022. – URL: https://www.rbc.ru/business/08/02/2022/620169fc9a794727f653e509 (дата обращения 20.03.2022).
4. Трудовой кодекс РФ. Статья 312.1. Общие положения [Электронный ресурс]. – 2020. – URL: http://www.consultant.ru/document/cons_doc_LAW_34683/adca37e8038a44ab5499c589bf6205dce6af12d6/ (дата обращения 15.03.2022).
5. Трудовой кодекс РФ Статья 214.2. Права работодателя в области охраны труда [Электронный ресурс]. – 2021. – URL: https://www.consultant.ru/document/cons_doc_LAW_34683/441967302a674ca7126cbc968e1e789100f5b0bd/? (дата обращения 15.03.2022).
6. Трудовой кодекс РФ Статья 15. Трудовые отношения [Электронный ресурс]. – 2006. – URL: http://www.consultant.ru/document/cons_doc_LAW_34683/823fdde09a529d3735916aa9fc1fe8d29ee04afb/ (дата обращения 15.03.2022).
7. Принципы работы StaffCop [Электронный ресурс]. – 2022. – URL: https://www.staffcop.ru/enterprise (дата обращения 17.05.2022).

8. Система контроля и учета рабочего времени сотрудников Kickidler [Электронный ресурс]. – 2022. – URL: https://www.kickidler.com/ru/ (дата обращения 18.05.2022).
9. Обзор Toptracker [Электронный ресурс]. – 2022. – URL: https://www.toptal.com/tracker (дата обращения 20.05.2022).
10. Стоимость лицензий Kickidler [Электронный ресурс]. – 2022. – URL: https://www.kickidler.com/ru/price.html (дата обращения 18.05.2022).
11. Купить StaffCop Enterprise [Электронный ресурс]. – 2022. – URL: https://www.staffcop.ru/buy/ (дата обращения 17.05.2022).
12. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов // 3-е изд., перераб. и доп. – М. : ФОРУМ, 2010. – 432 с.
13. C# documentation. Learn how to write any application using the C# programming language on the .NET platform [Электронный ресурс]. – 2023. – URL: https://learn.microsoft.com/en-us/dotnet/csharp/ (дата обращения 10.01.2023).

ORGANIZATION EMPLOYEES REMOTE WORK MONITORING SYSTEM DEVELOPMENT IN ORDER TO INCREASE THE LEVEL OF INFORMATION SECURITY

A.E. Golovchenko, Information security specialist
e-mail: dremartstud@gmail.com

The article studied and reviewed the current remote work control systems to identify the minimum required set of functionality for the development of such a system. A remote work monitoring system has been developed to record working hours, collect data on open processes, network activity and resource allocation of a working computer, which creates a timeline of an employee's work (the time spent in a certain window and how many times it was opened). The above set of functionality is designed to increase the level of information security of the organization.

Keywords: *development of a remote work control system, remote employees, increasing the level of information security of remote work, remote work control system*