УДК *004.056.53*

С. П. Серёдкин, В. А. Лисицын

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ В СИСТЕМАХ SCADA С ПОДДЕРЖКОЙ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. *В современном мире, где все больше устройств становятся подключенными к интернету, в том числе и системы управления промышленными процессами, возникает необходимость обеспечения их безопасности. Системы диспетчерского управления и сбора данных (SCADA) позволяют промышленным организациям контролировать данные и производственные процессы в режиме реального времени.*

Внедрение систем SCADA на предприятиях имеет множество преимуществ, которые позволяют увеличить эффективность и производительность производственных процессов, снизить затраты на производство, улучшить контроль над производственными процессами, повысить безопасность на предприятии и улучшить управление предприятием. Внедрение технологии интернета вещей в системы SCADA является важным шагом в развитии современных производственных технологий и помогает предприятиям стать более эффективными, повышать свою прибыльность и минимизировать простои на производстве. В противовес этому, с увеличением количества устройств, подключенных к интернету, возникает необходимость обеспечения безопасности систем управления промышленными процессами. В статье описываются основные угрозы, связанные с использованием систем SCADA с поддержкой интернета вещей, и методы защиты от этих угроз. Рассмотрена актуальность подобных систем, необходимость их защиты и основные методы, позволяющие повысить уровень безопасности на предприятии.

Результаты, полученные в ходе исследования, позволяют рассмотреть возможности интеграции систем SCADA и технологии интернета вещей, обратить внимание на основные моменты обеспечения безопасности таких систем и определить порядок мероприятий, необходимых для защиты производственных процессов.

Ключевые слова: *система диспетчерского управления, интернет вещей, безопасность на производстве, защита информации, SCADA, IoT, уязвимость, кибербезопасность.*

S. P. Seredkin, V. A. Lisitsyn

Irkutsk State Transport University, Irkutsk, the Russian Federation

IMPROVING SECURITY IN SCADA-ENABLED SYSTEMS INTERNET OF THINGS

Abstract. *In the modern world, where more and more devices are becoming connected to the Internet, including industrial process control systems, there is a need to ensure their security. Dispatch control and Data Acquisition (SCADA) systems allow industrial organizations to monitor data and production processes in real time.*

The introduction of SCADA systems at enterprises has many advantages that can increase the efficiency and productivity of production processes, reduce production costs, improve control over production processes, increase enterprise safety and improve enterprise management. The introduction of Internet of Things technology into SCADA systems is an important step in the development of modern production technologies and helps enterprises to become more efficient, increase their profitability and minimize production downtime. In contrast, with the increase in the number of devices connected to the Internet, there is a need to ensure the security of industrial process control systems. The article describes the main threats associated with the use of Internet-enabled SCADA systems and methods of protection against these threats. The relevance of such systems, the need for their protection and the main methods to increase the level of security at the enterprise are considered.

The results obtained in the course of the study allow us to consider the possibilities of integrating SCADA systems and Internet of Things technology, pay attention to the main points of ensuring the safety of such systems and determine the order of measures necessary to protect production processes.

Keywords: *dispatch control system, Internet of Things, safety at work, information protection, SCADA, IoT, vulnerability, cybersecurity.*

Введение

Безопасность в энергетической промышленности является важнейшим аспектом современного общества. Системы диспетчерского управления и сбора данных (SCADA) широко

используются в промышленном секторе для мониторинга и управления процессами [1]. С растущей интеграцией интернета вещей возникают новые возможности и вызовы, особенно с точки зрения кибербезопасности [2]. В данном исследовании обсуждается важность кибербезопасности в системах SCADA и шаги, которые необходимо предпринять для обеспечения их защиты.

Актуальность темы исследования обусловлена тем, что многие производственные отрасли стали нуждаться в SCADA-системах четвертого поколения с технологией интернет вещей [3]. В свою очередь, подобная технология помимо имеющейся массы положительных качеств, предлагает новые типы уязвимостей, которые необходимо принимать во внимание при построении системы обеспечения информационной безопасности.

Целью исследования является изучение влияния технологии интернета вещей (IoT) на системы SCADA (Supervisory Control and Data Acquisition), используемые для управления и контроля промышленных процессов.

Задачи исследования:

1. Изучить особенности технологии IoT и ее применение в промышленности.
2. Изучить особенности систем SCADA и их использование в промышленности.
3. Изучить возможности интеграции технологии IoT в системы SCADA.
4. Изучить преимущества и недостатки интеграции технологии IoT в системы SCADA.
5. Изучить потенциальные риски и угрозы, связанные с использованием технологии IoT в системах SCADA.
6. Разработать рекомендации по использованию технологии IoT в системах SCADA с целью повышения эффективности и безопасности промышленных процессов.

Интеграция технологии интернета вещей в системы SCADA

SCADA – это система мониторинга, которая используется для удаленного наблюдения и управления производственными процессами. Это один из типов промышленных систем управления, в частности, систем, использующихся для проектов с географически распределенными ресурсами. Системы на основе SCADA в большей степени ориентированы на сбор данных и являются частью АСУ ТП [4].

Интернет вещей же в свою очередь относится к физическим устройствам, которые обмениваются данными через цифровую сеть. Используя датчики и исполнительные устройства в оборудовании, интернет вещей собирает данные о том, как они функционируют. Внедряя технологию интернета вещей в продукт, становится возможным осуществлять удаленный мониторинг и управлять им, собирать данные о его работе и использовать эти их для улучшения продукта или создания новых функций [5].

Устройства интернета вещей все чаще интегрируются в системы SCADA для повышения их возможностей и эффективности. Интернет вещей обеспечивает ряд преимуществ [6]:

• предоставление непрерывных и точных данных о производительности оборудования и условиях окружающей среды, что позволяет лучше принимать решения и распределять ресурсы;

• осуществление удаленного мониторинга и управление промышленной инфраструктурой, уменьшение потребности в персонале на месте производства и обеспечение более быстрого реагирования на инциденты;

• обнаружение аномалий в производительности оборудования, обеспечение упреждающего обслуживания и снижение рисков сбоя и простоя;

• более тщательный мониторинг работы устройств без привязки к географическому положению оборудования.

Риски при внедрении интернета вещей в системы SCADA

Несмотря на потенциальные преимущества интернета вещей в системах SCADA, расширение возможностей подключения и зависимость от цифровых технологий также создают новые риски кибербезопасности. Промышленная инфраструктура является главной целью для кибератак из-за ее стратегической важности и потенциала крупномасштабных сбоев. Не-

которые из ключевых проблем кибербезопасности в системах SCADA с поддержкой интернета вещей включают [7]:

• расширение потенциальных точек входа для кибератак;

• необходимость защиты больших объемов данных, генерируемых устройствами интернета вещей;

• ограниченная вычислительная мощность и память устройств, затрудняющая внедрение надежных мер безопасности

• нехватка регулярных обновлений безопасности, приводящих к появлению уязвимостей.

В большинстве систем SCADA имеется специальная ЭВМ для управления и мониторинга системы. Сотрудники предприятия работают с системой при помощи интерфейса между вычислительной машиной и оператором или как их называют, человеко-машинным интерфейсом. Эти интерфейсы имеют решающее значение для взаимодействия с системой, но в тоже время могут служить критическим направлением для атак злоумышленников. Если злоумышленник получит доступ к интерфейсам, он фактически может взломать всю промышленную сеть.

Человеко-машинные интерфейсы, как правило, представляют собой системы на базе Windows с уникальным программным обеспечением, подключенным для управления и просмотра всех бизнес-систем [8]. Исходя из этого, можно понять, что программное обеспечение SCADA так же уязвимо для программных уязвимостей, как и любое программное обеспечение Windows. Получение злоумышленником доступа к человеко-машинному интерфейсу, может привести к полному овладеванию промышленным сектором, которым управляет система, после чего неизвестные вредоносные действия могут охватить промышленную сеть, к примеру, отключение датчиков и сигналов тревоги, повышение температуры и напряжения, изменение комбинации и концентрации химических веществ и т. п.

Основные меры обеспечения безопасности SCADA IoT

Важной концепцией, внедренной в автоматизацию процессов, являются зоны безопасности. Концепция зон безопасности классифицирует сегмент сети и определяет хосты и приложения с различными уровнями безопасности. Хосты и устройства в производственной зоне с высоким уровнем безопасности помещаются в одну зону, защищенную брандмауэром, и эти хосты взаимодействуют с другими хостами только после безопасной аутентификации.

Помимо определения требуемых зон, важно определить план IP для системы. План IP будет содержать имена хостов, IP-адреса и дополнительную информацию для всех хостов в системе, включая зону, в которой находится устройство с системой. Таким образом, можно использовать распределённую архитектуру для повышения безопасности отдельных сегментов сети [9].

Протоколирование событий, связанных с безопасностью, может быть очень полезным для захвата и записи событий, связанных с компонентами системы и активности пользователей для обзора и анализа. В системной сети можно регистрировать как успешные действия, так и неудачные попытки аутентификации или получения доступа к ресурсам системы, и эти записи журнала могут быть интегрированы с внешними функциями безопасности для безопасного хранения и анализа.

Для поддержания безопасности устройств интернета вещей, нельзя упускать из виду важную вещь - их своевременное и актуальное обновление. Во многих случаях могут возникать уязвимости, которые киберпреступники используют для развертывания своих атак. Важно, чтобы использовались последние обновления.

Что настоятельно рекомендуется сделать, так это изменить заводские настройки. Под этим подразумевается название устройства, а также любая информация, которая может быть общей и использоваться хакерами для развертывания своих атак. Необходимо изменить заводские настройки и не оставлять те, которые используются по умолчанию при покупке устройства.

Большинство устройств интернета вещей поставляются с заводскими паролями. Их также рекомендуется изменить, чтобы обеспечить необходимый уровень безопасности и избежать проблем.

Желательно также пересмотреть настройки конфиденциальности на устройствах интернета вещей, эти разрешения установлены по умолчанию и действительно открыты для сбора всех видов информации, включая ту, что может не использоваться системой, поэтому рекомендуется ее ограничить.

Также необходимо обратить внимание на место, где установлено соединение с системой и устройствами. Мы должны защитить доступ к этим устройствам извне.

Кроме того, необходимо создать дополнительную сеть Wi-Fi только для устройств интернета вещей [10], к которым не будет подключаться какое-либо оборудование с важной информацией, такое как компьютеры, смартфоны или планшеты. Это изолирует эти устройства, и система избежит возможных проблем, которые могут повлиять на другие устройства.

Наконец, рабочая сеть должна быть должным образом защищена. Необходимо использовать надежное шифрование, проверять используемый трафик сети и использовать надёжные пароли как для конфигурации оборудования, так и для беспроводной сети.

Исходя из вышеперечисленных разрозненных методов обеспечения безопасности можно выделить несколько основных принципов, которыми следует руководствоваться при реализации системы безопасности SCADA с поддержкой интернет вещей[11].

1. Определение и идентификация подозрительного поведения (идентификация).

При построении системы безопасности прежде всего необходимо определить, какое состояние промышленной сети будет являться нормальным. Поэтому для определения базового состояния системы необходимо провести инвентаризацию активов и потоков данных. Важным шагом на этом этапе является составление списка сетевого оборудования, используемых датчиков и устройств, а также IP-карты, для понимания и отслеживания потоков данных, передаваемых с помощью устройств интернета вещей. На этом моменте существенно облегчить задачу могут специализированные инструменты контроля сетевого оборудования, в которых присутствует функция построения карты сетевого оборудования и его контроля [12].

В случае использования устройств интернета вещей данные в большинстве случаев передаются по беспроводным сетям. Системы мониторинга могут позволить отслеживать изменения IP-адресов, изменение положения устройств и выявлять несанкционированные подключения или утечку данных. Особенно это касается мобильных датчиков, которые часто передают данные через WI-FI точки доступа с динамическим IP-адресом, который довольно сложно мониторить не прибегая к специальным инструментам.

2. Защита внутренней сети (защита)

Сложность пароля является одним из ключевых факторов, влияющих на безопасность системы. Чем сложнее пароль, тем выше вероятность, что он будет устойчив к взлому. Исследования показывают, что использование длинных и сложных паролей, состоящих из букв, цифр и специальных символов, может значительно повысить уровень безопасности системы. Например, пароль длиной 12 символов, состоящий из букв, цифр и специальных символов, может быть взломан только при использовании мощного компьютера и специальных программ. Однако, многие пользователи предпочитают использовать простые пароли, такие как "password" или "123456", что делает их уязвимыми для атак взломщиков. Подобные пароли предоставляют потенциальные точки входа в систему, позволяя злоумышленнику при должной сноровке и ослабленной системе безопасности годами находиться в промышленной сети, распоряжаясь получаемой информацией или подготавливаясь к крупномасштабному удару по SCADA [13]. Причём стоит уточнить, что не только учётные записи администраторов подвержены риску взлома. Как правило, хакеры нацелены на все классы пользователей, включая тех, у кого минимальные полномочия. Поэтому, для повышения безопасности системы необходимо регулярно обучать пользователей созданию сложных паролей и использованию двухфакторной аутентификации, а также настроить парольную политику, удовле-

творяющую требованиям надёжности паролей. То же касается основных учётных данных устройств интернета вещей, включающих в себя стандартную информацию об устройствах и паролях, которых нужно заменить при первой же возможности. Разумеется, все конфигурационные файлы и потоки данных должны шифроваться, а подключения использовать защищенные протоколы, такие как HTTPS.

Отдельно стоит выделить управление политиками безопасности, включающее в себя предоставление ресурсов в зависимости от рабочей зоны и жёсткое ограничение доступа к данным системы, базирующееся на географической основе. Важно постоянно мониторить состояние и своевременно отключать неиспользуемые учётные записи пользователей. Далеко не редкость ситуации, когда уже не участвующий в работе системы сотрудник всё ещё имеет к ней доступ и имеет потенциальную возможность нанести ущерб предприятию используя свою учётную запись.

Помимо этого, стоит обратить внимание на своевременное обновление устройств интернета вещей, предоставление последних версий данных и как можно быструю реакцию на обнаруживаемые уязвимости в системе. Нередки случаи, когда после обнаружения уязвимости в системе ещё несколько месяцев не принимается никаких действий по её устранению, чего вполне хватает для реализации атаки на систему SCADA и причинению ущерба производственной сети.

3. Мониторинг подозрительного поведения (обнаружение).

После определения базового состояния системы, инвентаризации активов и потоков данных системы, можно сказать, что мы понимаем, как система работает в нормальном режиме. С помощью специализированного программного обеспечения можно построить базовые шаблоны состояния системы и, сравнивая их с текущим состоянием, говорить о том, имеются ли аномалии в работе промышленной сети.

4. Принятие действий на основе сигнала тревоги (реагирование).

В случае присутствия аномалий в работе система должна генерировать сигналы тревоги, а персонал реагировать на выявленные аномалии, выполняя воздействие на конкретный случай установленного нестандартного поведения. Важным шагом на этом этапе является изоляция инцидента. Необходимо изолировать инцидент, чтобы предотвратить дальнейшее распространение вируса или злоумышленной атаки. Это может включать отключение системы от сети или временное отключение доступа пользователей [14].

Для устройств интернета вещей необходимо предусмотреть сценарий работы в случае обнаружения вторжения или аномалий включающий в себя либо блокировку устройства, либо стирание его информации, перезагрузку, возвращение к последней безопасной конфигурации или же отключения от сети. Важно понимать, что необходимо хранить прошлые версии программного обеспечения и драйверов, чтобы в случае критической неисправности или обнаружения уязвимости вернуть устройство к последнему стабильному состоянию. Исходя из этого мы приходим к необходимости ведения журнала версий для поддержания целостности конфигурации системы и отслеживания истории изменений системы в общем и её компонентов, в частности.

5. Восстановление работы системы после инцидента безопасности (восстановление).

Как бы не было всё хорошо по плану, в действительности, при обнаружении критической неисправности или вторжения злоумышленника в промышленную систему реагирование на инцидент безопасности или восстановление работоспособности системы в некоторых случаях может занять продолжительное время. Для избежание простоев или потери исторических данных системы применяется технология резервирования, позволяющая создавать дополнительные сети и сервера для их запуска в случае нарушения работоспособности основной промышленной сети. Подобная технология может быть реализована посредством виртуальных серверов, используемых в качестве хостов, на которых хранится последняя работоспособная версия системы. Помимо самой системы, обычно резервирование используется в качестве меры защиты накопленной информации, посредством синхронизации баз данных и периодического обновлением информации на резервных виртуальных машинах [15]. В

случае нарушения работоспособности сети это не только позволит сохранить исторические данные системы, но и продолжить работу, временно переместившись с основной сети в резервную.

Что касается основной сети, необходимо оценить ущерб, который был нанесен системе в результате инцидента безопасности. Это может включать потерю данных, повреждение системных файлов, нарушение конфиденциальности и другие проблемы, после чего восстановить работу системы посредством принятия мер в зависимости от конкретного инцидента, которые могут включать в себя обновление программного обеспечения, изменение паролей и настройку дополнительных мер защиты и т. п.

Заключение

В заключение можно сказать, что использование технологий интернета вещей в промышленности может значительно улучшить производственные процессы и повысить эффективность работы предприятий. Однако, это также может привести к дополнительным рискам информационной безопасности. Важно понимать, что любое устройство, подключенное к интернету, может стать объектом кибератак. Промышленные системы управления могут быть особенно уязвимыми, так как они подключены к большому количеству устройств и имеют доступ к критической информации. Для обеспечения безопасности интернета вещей в промышленности необходимо использовать надежные методы аутентификации и шифрования данных, а также мониторить сетевую активность для выявления аномалий и инцидентов. Кроме того, необходимо обучать сотрудников правилам безопасности и проводить регулярный анализ на наличие уязвимостей.

В целом, использование технологий интернета вещей в промышленности может принести множество преимуществ, но только при условии обеспечения надежной защиты от кибератак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. SCADA - назначение систем [Электронный ресурс] // TADVISER. 2020. 26 июня – URL: https://www.tadviser.ru/index.php/Статья:SCADA_назначение_систем (дата обращения: 09.05.2023).
2. Проблемы безопасности интернета вещей и передовые методы их решения [Электронный ресурс] // Kaspersky – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security (дата обращения: 08.05.2023).
3. Кондратьев В. Б. Четвертая промышленная революция и глобализация // Перспективы. Электронный журнал. 2018. № 2 (14). – С. 92-108.
4. Ю. В. Константинов, В. Г. Некрутов, В. Д. Константинов Анализ современных SCADA-систем // Секции технических наук: материалы 67-й науч. конф. 2015. С. 1734-1740.
5. Перри Ли Архитектура интернета вещей // ДМК Пресс. 2019. – 456 с.
6. Промышленный интернет вещей [Электронный ресурс] // СОФТЕЛ. – URL: https://sofiot.ru/promyshlennyj-internet-veshhej (дата обращения: 12.05.2023).
7. Верещагина Е.А., Капецкий И.О., Ярмонов А.С. Проблемы безопасности Интернета вещей // М.: Мир науки. 2021. – 105 с.
8. Ямалтдинова Э. И. Человеко-машинный интерфейс // Достижения науки и образования. 2020. – 3 с.
9. Информационная безопасность интернета вещей [Электронный ресурс] // TADVISER. 2023. 27 марта – URL: https://www.tadviser.ru/index.php/ Статья:Информационная_безопасность_интернета_вещей_(Internet_of_Things) (дата обращения: 16.05.2023).
10. Информационная безопасность в IoT [Электронный ресурс] // habr. 2022. 28 ноября – URL: https://habr.com/ru/articles/700800/ (дата обращения: 16.05.2023).
11. Концепция совершенствования кибербезопасности критически важной инфраструктуры - Дополнительные материалы к докладу на конференции «IT Security Conference 2019» // Перевод. г. Минск, 2019. – 64 с.

12. Эд Ньюджент, Майк Рэтт Обеспечение кибербезопасности SCADA в эпоху «Интернета вещей» // Control Engineering Россия Апрель 2017. – 3 с.

13. Ключи для умных устройств: какие сочетания логинов и паролей чаще всего вводят злоумышленники [Электронный ресурс] // Kaspersky – URL: https://www.kaspersky.ru/about/press-releases/2022_klyuchi-dlya-umnyh-ustrojstv-kakie-sochetaniya-loginov-i-parolej-chashe-vsego-vvodyat-zloumyshlenniki (дата обращения: 23.05.2023).

14. Реагирование на инциденты: основные этапы и ошибки. [Электронный ресурс] // alfastrah – URL: https://ir.alfastrah.ru/posts/629 (дата обращения: 23.05.2023).

15. Питкевич П.И. Методы резервирования данных для критически важных ИТ-систем предприятия // Universum: технические науки : электрон. научн. журн. 2021. 10(91) URL: https://7universum.com/ru/tech/archive/item/12405 (дата обращения: 27.05.2023).

REFERENCES

1. SCADA - naznachenie sistem [Elektronnyi resurs] // TADVISER. 2020. 26 iiunia – URL: https://www.tadviser.ru/index.php/Stat'ia:SCADA_naznachenie_sistem (data obrashcheniia: 09.05.2023).

2. Problemy bezopasnosti interneta veshchei i peredovye metody ikh resheniia [Elektronnyi re-surs] // Kaspersky – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security (data obrashcheniia: 08.05.2023).

3. Kondrat'ev V. B. CHetvertaia promyshlennaia revoliutsiia i globalizatsiia // Perspektivy. Elek-tronnyi zhurnal. 2018. no 2 (14). pp. 92-108.

4. IU. V. Konstantinov, V. G. Nekrutov, V. D. Konstantinov Analiz sovremennykh SCADA-sistem // Sektsii tekhnicheskikh nauk: materialy 67-i nauch. konf. 2015. S. 1734-1740.

5. Perri Li Arkhitektura interneta veshchei // DMK Press. 2019. 456 p.

6. Promyshlennyi internet veshchei [Elektronnyi resurs] // SOFTEL. URL: https://sofiot.ru/promyshlennyj-internet-veshhej (data obrashcheniia: 12.05.2023).

7. Vereshchagina E.A., Kapetskii I.O., IArmonov A.S. Problemy bezopasnosti Interneta veshchei // Moskva: Mir nauki. 2021. 105 p.

8. IAmaltdinova E. I. CHeloveko-mashinnyi interfeis // Dostizheniia nauki i obrazovaniia. 2020. 3 p.

9. Informatsionnaia bezopasnost' interneta veshchei [Elektronnyi resurs] // TADVISER. 2023. 27 marta – URL: https://www.tadviser.ru/index.php/ Sta-t'ia:Informatsionnaia_bezopasnost'_interneta_veshchei_(Internet_of_Things) (data obrashcheniia: 16.05.2023).

10. Informatsionnaia bezopasnost' v IoT [Elektronnyi resurs] // habr. 2022. 28 noiabria – URL: https://habr.com/ru/articles/700800/ (data obrashcheniia: 16.05.2023).

11. Kontseptsiia sovershenstvovaniia kiberbezopasnosti kriticheski vazhnoi infrastruktury - Dopolnitel'nye materialy k dokladu na konferentsii «IT Security Conference 2019» // Perevod. g. Minsk, 2019. 64 p.

12. Ed N'iudzhent, Maik Rett Obespechenie kiberbezopasnosti SCADA v epokhu «In-terneta ve-shchei» // Control Engineering Rossiia Aprel' 2017. 3 p.

13. Kliuchi dlia umnykh ustroistv: kakie sochetaniia loginov i parolei chashche vsego vvodiat zlo-umyshlenniki [Elektronnyi resurs] // Kaspersky – URL: https://www.kaspersky.ru/about/press-releases/2022_klyuchi-dlya-umnyh-ustrojstv-kakie-sochetaniya-loginov-i-parolej-chashe-vsego-vvodyat-zloumyshlenniki (data obrashcheniia: 23.05.2023).

14. Reagirovanie na intsidenty: osnovnye etapy i oshibki. [Elektronnyi resurs] // alfastrah – URL: https://ir.alfastrah.ru/posts/629 (data obrashcheniia: 23.05.2023).

15. Pitkevich P.I. Metody rezervirovaniia dannykh dlia kriticheski vazhnykh IT-sistem predpriia-tiia // Universum: tekhnicheskie nauki : elektron. nauchn. zhurn. 2021. 10(91) URL: https://7universum.com/ru/tech/archive/item/12405 (data obrashcheniia: 27.05.2023).

Информация об авторах

Серёдкин Сергей Петрович - к.э.н. доцент кафедры ИСиЗИ, Иркутский государственный университет путей сообщения, г. Иркутск

Лисицын Владислав Александрович - студент группы БИм.1-22-1, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: vladlisitsindiklis@yandex.ru

Information about the authors

Seredkin Sergey Petrovich – candidate of technical Sciences,Associate Professor,Associate Professor of the Department "Information systems and information protection", Irkutsk State Transport University, Irkutsk

Lisitsyn Vladislav Alexandrovich – student of the BIm group.1-22-1, Irkutsk State Transport University, Irkutsk