предохраняя его от взрыва с последующим разрушением и загрязнением окружающей среды радиоактивными элементами. Таким образом, обеспечивается дальнейшее повышение надежности и живучести АЭС, так как простота конструкции насосов инжекторного типа, отсутствие механического привода насосов обеспечивает их исключительную надежность.

В результате может быть обеспечено повышение надежности, живучести и безопасности работы АЭС. С учетом уже имеющегося опыта в атомной энергетике ликвидация аварий АЭС с ядерным реактором требует десятилетий и материальных затрат на сумму в сотни млрд долларов США.

Литература:

1. *Лещенко В.В.* Повышение технической безопасности сложных систем с ядерным реактором / Проблемы управления безопасностью сложных систем: материалы XXVIII Международной конференции. 16 декабря 2020 г., Москва. – Москва: ИПУ РАН, 2020. – С. 276-280.

2. Атомная электрическая станция: патент на изобретение № 2638304 Российская Федерация / Лещенко В.В. Заявка № 2016152733 от 30.12.2016. Опубликовано: 13.12.2017. Бюллетень № 35.

DOI: 10.25728/iccss.2023.50.49.032

Баранов Л.А., Ермакова А.Е., Иконников С.Е.

Информационная безопасность систем диспетчерского управления на железнодорожном транспорте

Аннотация: В работе рассмотрены основные методы защиты информации в телемеханических системах на железнодорожном транспорте, определены принципы информационной безопасности в системах диспетчерского управления, обоснована необходимость комплексного подхода к защите данных таких систем.

Ключевые слова: информационная безопасность**,** системы диспетчерского управления, внутренняя локальная сеть,

защита периметра сети, инциденты информационной безопасности

Комплексные системы управления на железнодорожном транспорте объединяют системы локального и телемеханического управления. На современном уровне разработки таких систем используются алгоритмы интеллектуального управления [1].

Рассмотрим особенности обеспечения информационной безопасности в системах телемеханического управления, устройств энергоснабжения электрифицированных железных дорог и в системах диспетчерской централизации – телеуправления-телесигнализации стрелками и сигнализацией.

Использование при передаче сигналов управления и приеме телесигналов каналов связи, которые могут быть атакованы злоумышленниками, обуславливает необходимость разработки алгоритмов защиты информации в этих условиях.

В этом случае, учитывая, что контроль осуществляется стационарным устройством, следует использовать защиту, минимизирующую вероятность преобразования кодовых комбинаций и допускающую некоторое увеличение вероятности сбоя декодирования. Такой подход возможен при использовании вычислительных средств на пунктах диспетчеризации и контроля.

На рисунке 1 представлены основные методы защиты информации в телемеханических системах на железнодорожном транспорте.

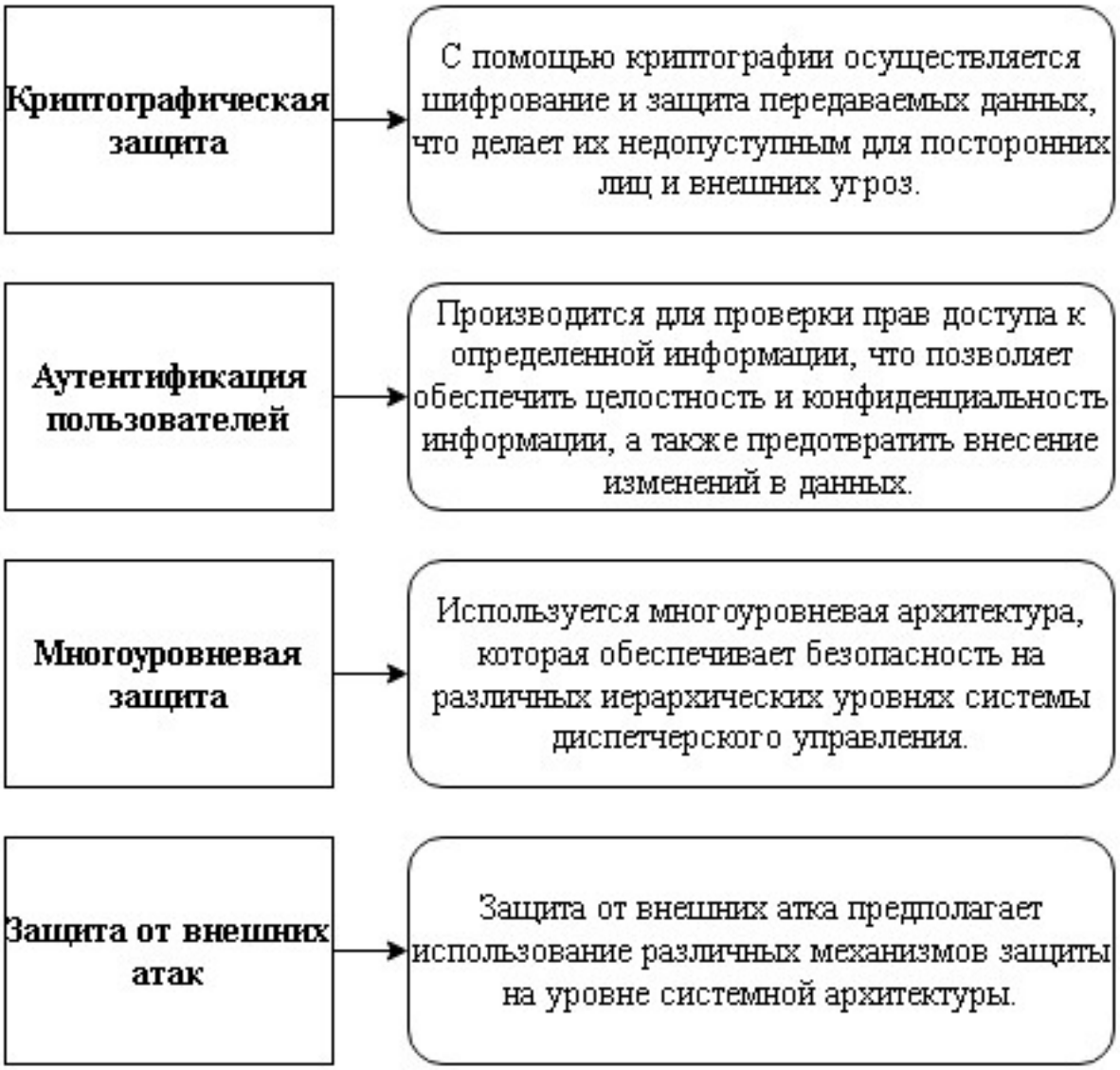

Рисунок 1 – Основные методы защиты информации в телемеханических системах на железнодорожном транспорте

Если к системе диспетчерского управления подключаются внешние сетевые ресурсы, то требуется предусмотреть следующее:

– защиту внутренней сети от удаленного несанкционированного доступа из внешних сетей;

– сокрытие информации о структуре внутренней сети и ее компонентов от пользователей внешней сети;

– разграничение доступа из внешних сетей к защищенной внутренней сети и доступа из защищенной сети во внешнюю сеть.

Для минимизации возникновения угроз информационной безопасности в системах мониторинга и управления должен

осуществляться постоянный мониторинг оборудования, имеющего доступ к внешним сетям [3].

Предприятиям железнодорожного транспорта, эксплуатирующим системы диспетчерского управления, необходимо провести аудит всего оборудования, доступного из внешних сетей, или обратиться к аккредитованным специалистам для устранения уязвимостей и самотестирования такого оборудования.

С учетом статистики инцидентов нарушения информационной безопасности в автоматизированных системах на железнодорожном транспорте отмечен значительный рост числа атак на защищенные сети таких систем, при этом увеличилось количество опасных программ и сервисов в открытом доступе, что определяет необходимость в применении комплексных систем защиты информации [4].

Вероятными направлениями атаки злоумышленников с целью получения несанкционированного доступа в систему диспетчерского управления могут быть:

– маршрутизаторы на границе внутренней сети;
– устаревшие и/или анонимные учетные записи пользователей;
– сервисы электронной почты;
– съемные носители информации.

С целью обеспечения высокого уровня защиты информации в системах диспетчерского управления на железнодорожном транспорте необходимо придерживаться следующих принципов:

1. сегментирования внутренней локальной сети, в которую входит система диспетчерского управления;
2. анализа трафика в такой локальной сети;
3. создания доверенного аппаратно-программного комплекса (в части операционных систем, прикладного программного обеспечения, прошивки микроконтроллеров, базовой системы ввода-вывода);
4. обязательного применения средств криптографии (закрытого кода);
5. создания изолированной среды для запуска только одного приложения, создаваемой средствами на уровне ядра операционной системы (контейнеризация).

Указанные принципы отражают комплексный подход к информационной безопасности для систем диспетчерского управления на железнодорожном транспорте, реализация которого позволит:

– управлять инцидентами информационной безопасности, организовать и группировать их корреляцию и сократить время обработки;

– организовать облачную инфраструктуру с настраиваемыми сервисами безопасности, разработку и внедрение программных и аппаратных средств, в том числе локальных установок для хранения всех данных в пределах периметра защищенной сети.

Вывод

Системы диспетчерского управления являются ключевым элементом современного железнодорожного транспорта, они обеспечивают безопасное и надежное управление перевозочным процессом. С развитием технологий обработки данных на железнодорожном транспорте возрастает риск угроз информационной безопасности, что может привести к серьезным негативным последствиям и нарушениям в работе транспортных предприятий. Обеспечение информационной безопасности систем диспетчерского управления на железнодорожном транспорте приведет к снижению количества инцидентов в инфраструктуре таких систем и минимизации их последствий, кроме того, повысится надежность и качество управления транспортными процессами.

Литература:

1. *Баранов Л.А., Балакина Е.П., Иконников С.Е., Антонов Д.А.* Централизованное управление движением поездов городских железных дорог современного мегаполиса // Наука и техника транспорта. – 2020. – № 1. – С. 30-38.

2. *Иконников С.Е., Ермакова А.Е.* Построение защищенной локальной сети организации на основе межсетевого экранирования / Материалы Международной научно-практической конференции «Интеллектуальные транспортные системы». Москва, 26 мая 2022 года. – М.: Российский университет транспорта, 2022. – С. 187-192.

3. *Иконников С.Е.* Комплексная система защиты на объектах критической информационной инфраструктуры / Материалы II Международной научно-практической конференции «Интеллектуальные транспортные системы». Москва, 25 мая 2023 года. – М.: Российский университет транспорта, 2023. – С. 475-477.

4. *Ермакова А.Е., Иконников С.Е.* Требования по информационной безопасности для автоматизированных систем диспетчерского управления на транспорте / Proceedings XV međunarodni naučno-stručni skup Informacione Tehnologije za e-Obrazovanje ITeO. 29-30.9.2023, Banja Luka. – Banja Luka: Panevropski univerzitet Apeiron, 2023. – P. 162-166.

DOI: 10.25728/iccss.2023.53.91.033

Баранов Л.А., Михалевич И.Ф., Иванова Н.Д., Соколов С.С.

Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз

Аннотация: В работе рассмотрена проблема обеспечения информационной безопасности как интегрированной автоматизированной системы корпоративного и технологического управления. Рассмотрен вариант управления рисками информационной безопасности системы автономного судовождения с использованием технологий дополненного интеллекта и модели системы мониторинга сложных процессов.

Ключевые слова: безопасность транспорта, свойство подлинности информации, промышленная криптография, экспертная оценка, теория нечетких множеств

Введение

С развитием технологий транспортные средства перестали являться самостоятельными объектами, и в соответствии с принципом V2X (Vehicle-to-Everytning) взаимодействуют с другими транспортными средствами, транспортной инфраструктурой и любыми другими объектами, которые могут повлиять на их