УДК 621.31

МОДЕРНИЗАЦИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССОВ СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

А. Ю. КОВАЛЬЧУК
Белорусская железная дорога, г. Минск

К. АДИБ МЕНЬКОВА
Белорусский государственный университет транспорта, г. Гомель

Информационная инфраструктура современной крупной или средней организации включает в свой состав сети передачи данных, серверное оборудование, системы виртуализации, разнообразное системное и прикладное и программное обеспечение, средства защиты информации, рабочие места пользователей и другие взаимодействующие друг с другом компоненты.

Современные реалии, процессы всеобщей информатизации и цифровизации неразрывно связаны с рисками нарушения информационной безопасности и возникновения киберинцидентов разных масштабов и разной степени тяжести.

Основным инструментом минимизации количества негативных цифровых воздействий на информационные системы, подключенные к открытым каналам передачи данных и обрабатывающие информацию, распространение и (или) предоставление которой ограничено, являются создание систем защиты информации с последующим прохождением, в случае необходимости, аттестации на соответствие установленным требованиям.

Наиболее ресурсозатратными и требующими специфических высокооплачиваемых компетенций мероприятиями, которые необходимо реализовать при создании систем защиты информации являются сегментация сети передачи данных и виртуальной среды, внедрение специализированных средств защиты информации (межсетевые экраны, системы обнаружения и предотвращения вторжений, антивирусное программное обеспечение и т. п.), обеспечение сбора и хранения журналов событий информационной безопасности (логов) всех элементов информационной системы и выстраивание процессов реагирования на события информационной безопасности, построение систем мониторинга и т. п.

Накопленный Белорусской железной дорогой опыт построения систем защиты информации информационных систем созданных (создаваемых) для автоматизации технологических и бизнес-процессов показывает, что принципы и подходы, заложенные в основу созданной более 10 лет назад информационной инфраструктуры, являются серьезным препятствием в реализации действенных мер по обеспечению кибербезопасности. На практике для создания эффективной (соответствующей требованиям регулятора) системы защиты информации приходится реализовывать масштабные и дорогостоящие мероприятия по изменению параметров, а в части случаев и архитектуры информационной инфраструктуры, которые в том числе включают в себя ее дооснащение или замену отдельных ее элементов.

Для экономии финансовых, трудовых и временных ресурсов на этапах создания систем защиты информации информационных систем целесообразно проработать возможность внедрения следующих подходов на этапах создания, модернизации и развития информационной инфраструктуры в составе которой будут функционировать информационные системы, подключенные к открытым каналам передачи данных и обрабатывающие информацию, распространение и (или) предоставление которой ограничено.

Меры, которые изолируют сегменты сети и сервисы, предотвращая горизонтальные перемещения злоумышленника и снижая риски кибератак. Разделение на пользовательские и технологические контуры дополнительно защищает критичные системы, минимизируя поверхность атак:

– физическая сегментация с использованием средств межсетевого экранирования между физическими сегментами (разделение сети на контуры) и внешними сетями;

– логическая сегментация (разделение сети на сервисы);

– разделение информационной инфраструктуры на пользовательские и технологические сегменты, минимизация количества внешних взаимодействий с технологическими сегментами.

Нижеперечисленные меры позволяют создать многоуровневую защиту, блокируя любые несанкционированные соединения между сегментами сети. Это предотвращает распространение атак даже в случае компрометации одного из элементов инфраструктуры, изолируя угрозу и минимизируя ущерб:

– использование принципа «запрещено всё, что не разрешено» при организации сетевых взаимодействий между контурами и сегментами сети;

– регламентация порядка использования IP-адресации с учетом исключения возможности взаимодействия между контурами и сегментами по умолчанию даже в случае их умышленного или неумышленного физического соединения;

– минимизация случаев прямого взаимодействия между рабочими станциями находящимся в разных сегментах посредством использования шлюзов в виде прокси-серверов, почтовых серверов, терминальных серверов и т. п.

Меры, которые создают автономный контур безопасности, который обеспечивает контроль над критичными сервисами, непрерывный мониторинг и восстановление системы даже в случае масштабной кибератаки:

– разделение распределенной системы доменных имен на внутренний и внешний контуры;

– обеспечение функционирования систем мониторинга средств вычислительной техники (включая серверы, системы хранения данных и т. п.), телекоммуникационного оборудования, системного программного обеспечения (включая программное обеспечения систем виртуализации и систем бэкпапирования) и средств защиты информации;

– создание автономных инструментов для хранения резервных копий наиболее критичных элементов информационной инфраструктуры с использованием принципа «воздушной прослойки» (физическая изоляция от других устройств и сетей).

Данный комплекс мер минимизирует зависимость от внешних поставщиков и снижает риск утечек, обеспечивая при этом многоуровневый контроль над всеми потенциально уязвимыми точками:

– минимизация использования проприетарных решений;

– минимизация участия в технологических и бизнес-процессах сторонних организаций, организация их опосредованного участия в случае необходимости;

– использование систем обнаружения и предотвращения вторжений;

– обеспечение контроля за внешними подключениями;

– обеспечение контроля за привилегированными пользователями;

– использование систем обеспечения обнаружения и предотвращения утечек информации;

– использование централизованной системы сбора информации и управления агентами защиты от воздействия вредоносных программ;

– использование систем автоматизированного анализа основных потоков информации;

– использование централизованной системы сбора, корреляции и хранения сведений о событиях информационной безопасности;

– обеспечение наличия и поддержания в актуальном состоянии структурных и логических схем объектов информационной инфраструктуры и другой документации.

На рисунке 1 представлена схема модернизации информационной безопасности на Белорусской железной дороге. Данная схема представляет собой сеть на основе межсетевых экранов, обеспечивающих защиту сети железной дороги от несанкционированного доступа из сети интернет. Сплошной линией отмечены уже существующие контуры и устройства, а пунктиром – запланированные. Планируется организация кластера межсетевых экранов для защиты от угроз из сетей сопредельных стран.

Использование перечисленных подходов позволит существенно повысить уровень кибербезопасности информационной инфраструктуры организации и, как следствие, избежать финансовых и репутационных потерь за счет сокращения количества и (или) уменьшения масштабов негативных цифровых воздействий (кибератак). Перечисленные выше подходы нашли практическое применение в реализуемом в настоящее время проекте по приведению одного из вычислительных комплек-

сов Белорусской железной дороги в соответствие с требованиями законодательства в сфере информационной безопасности.

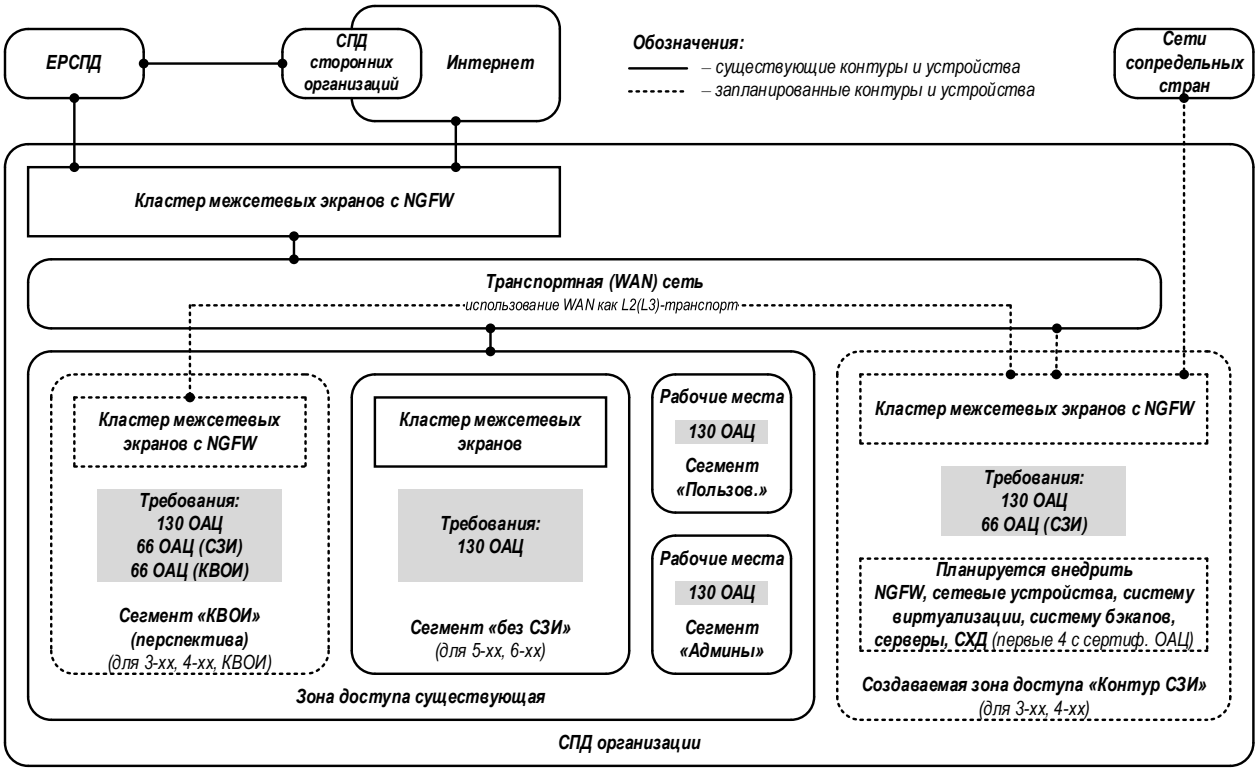

Рисунок 1

УДК 621.391.825

МОДЕЛЬ АНАЛИЗА И ПРОГНОЗИРОВАНИЯ ПОМЕХОУСТОЙЧИВОСТИ МИКРОПРОЦЕССОРНЫХ СЖАТ К ЭЛЕКТРОМАГНИТНЫМ ИМПУЛЬСАМ ПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ

Д. В. КОМНАТНЫЙ

Гомельский государственный технический университет им. П. О. Сухого, Республика Беларусь

На современном этапе развития научного направления «электромагнитная совместимость» внимание специалистов привлечено к проблеме защиты критически важных объектов от электромагнитных импульсов преднамеренного воздействия (ЭИПВ). Эта проблема начала обсуждаться в первые годы XXI века и с того времени приобретает все большую актуальность по причине обострения международной обстановки, возросшей террористической активности, появления доступных злоумышленникам низкого и среднего технического уровня малогабаритных генераторов ЭИПВ.

Современные микропроцессорные и компьютерные системы железнодорожной автоматики и телемеханики (СЖАТ), призванные обеспечивать безопасность движения поездов, также требуют защиты от ЭИПВ. Подтверждением этому является реализация в Евросоюзе проекта SECRET (**SE**-**C**urity of **R**ailways against **E**lectromagnetic a**T**tacks). Но в ограниченно опубликованных результатах работы по проекту описаны только исследования воздействия ЭИПВ на штатные антенны радиоэлектронных СЖАТ. Кроме этого пути, воздействие ЭИПВ может осуществляться непосредственно на аппаратуру СЖАТ внутри технических зданий по свободному пространству, по цепям питания и по интерфейсным линиям. Анализ нормативно-технической документации по проблеме защиты от ЭИПВ позволяет заключить, что воздействие по свободному пространству более доступно для злоумышленников низкого и среднего технического уровня. Генераторы ЭИПВ этого типа могут быть