ОПИСАНИЕ СИСТЕМЫ

В ходе выполнения конкурсного задания вам необходимо разработать модули системы защиты объекта критической информационной инфраструктуры (КИИ) на основе 187-ФЗ «О безопасности КИИ Российской Федерации».

Система безопасности объекта КИИ должна обеспечивать:

1) предотвращение неправомерного доступа к информации;
2) недопущение воздействия на технические средства обработки информации;
3) восстановление функционирования значимых объектов КИИ;
4) непрерывное взаимодействие с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются:

1) организация контроля физического доступа к значимому объекту;
2) реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации значимого объекта;
3) проверка полноты и детальности описания в организационно-распорядительных документах по безопасности значимых объектов действий пользователей и администраторов значимого объекта по реализации организационных мер;
4) отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.

Основная проблема объектов КИИ - атаки на критическую инфраструктуру

Реализация угроз может привести к прекращению или нарушению функционирования значимого объекта и обеспечивающего (управляемого, контролируемого) им процесса, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации). Как следствие – существенные, федерально значимые, последствия для жизни и здоровья людей, экологии, экономики.

При неправомерном отношении или воздействии на значимые объекты КИИ и процессы, система обеспечения информационной безопасности (СОИБ) фиксирует и реагирует на возникшие инциденты и стремится минимизировать последствия угроз безопасности.

Злоумышленники могут нарушить процессы работ КИИ Российской Федерации в организациях, например:

- с использованием вирусных программ для управления SCADA – систем (злоумышленник смог найти уязвимые места в системе безопасности и изменил настройки управления значимого объекта КИИ, что повлекло нарушение работы процессов АСУТП)
- нарушение целостности процессов объектов КИИ (сотрудник внёс изменения в код программного обеспечения значимого объекта КИИ, что повлекло нарушение передачи информации по информационно-телекоммуникационной сети).

Атаки могут совершать не только злоумышленники-хакеры. Разглашение сотрудниками субъектов КИИ сведений об объектах КИИ (даже просто перечень объектов, степень их значимости, последствия для объектов), либо неразрешенное изменение информации в них (отключение антивируса на сервере управления химическим реактором) – приравнивается к атаке.

Важно, что неправомерное воздействие на значимые объекты и процессы влечет за собой уголовную ответственность, содержащаяся в статье 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Таким образом, атаки на КИИ не только регулируются нормативными документами, но и караются в соответствии с уголовным кодексом.

В рамках выполнения конкурсного задания вам необходимо разработать:

1) модуль по организации контроля физического доступа к значимому объекту «ХранительПРО»;
2) модули централизованного мониторинга событий на рабочих станциях сотрудников объекта КИИ «Стражник».