ВЕКТОРЫ ИНСАЙДЕРСКИХ АТАК НА ЭЛЕМЕНТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ А.В. Федорцов

Критически важная информационная инфраструктура отдельно взятых организаций (производств) формирует уникальное пространство для развития инсайдерских атак (ИА) на элементы, эмулирующие информационные объекты (ИО) внутри сегментов соответствующих информационных сетей специального назначения (ИССН) [1, 2]. Такие ИССН, как правило, содержат особую конфигурацию структуры/функционала известных категорий средств: программно-технические средства (hardware); программные средства общего и прикладного назначения (software).

В качестве векторов ИА выступают уязвимости вышеназванных элементов ИССН, которые представляют собой частные цели для получения несанкционированного доступа и последующего несанкционированного воздействия на критические свойства ИО. В ходе ИА происходит эскалация привилегий инсайдера посредством эксплуатации уязвимостей элементов ИССН с применением exploit-инструментов/инструкций, полученных из DarkNet, от внешнего злоумышленника. Это приводит к нарушению установленных политик безопасности и реальному ущербу организации (производству) от воздействия на ИО.

Для решения задачи устранения уязвимостей элементов ИССН приоритетным способом следует использовать риск-ориентированный подход, основанный на методологическом аппарате количественной оценки потенциального ущерба от их эксплуатации инсайдером. Ее выполнению предшествует ранжирование по уровням опасности набора метрик уязвимостей software- и hardware-элементов, собранных из соответствующих баз и матриц безопасности программно-технических средств [2].

Литература

1. Федорцов А.В. Пути реализации атак на информационную инфраструктуру критически важных объектов Республики Беларусь // Управл. информац. ресурс.: матер. XIV Междунар. науч.-практ. конф., Минск, 20 декабря 2017 г. – С. 191–193.

2. Федорцов А.В. Матрица безопасности программно-технических средств защиты информации организации // Технич. средств. защит. инф.: тезис. докл. XVII Белорус.-российск. науч.-техн. конф., Минск, 11 июня 2019 г. – С. 71–72.