

***В.Е. Муценек***

*МГЛУ ЕАЛИ, ст. преп. кафедры информационных технологий*

## **УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ПРОТИВОБОРСТВА РОССИИ И ИНОСТРАННЫХ ГОСУДАРСТВ**

Агрессивная санкционная политика государств Европейского Союза и блока НАТО диктует необходимость дополнительной оценки угроз безопасности информации, обрабатываемой в российских информационных системах независимо от принадлежности таких систем государственному или частному секторам.

Доктрина информационной безопасности Российской Федерации, утверждённая задолго до ухудшения внешнеполитической обстановки, констатирует факт нехватки конкурентоспособной электронной продукции отечественного производства, в особенности программно-аппаратных средств.[1] В условиях продолжающихся попыток экономической и политической изоляции России зависимость отечественной индустрии информационных технологий от импортной продукции становится серьёзным поводом для беспокойства. Данная статья обобщенно представляет некоторые возможные сценарии нарушения защищенности отечественных информационных систем в условиях международного противоборства.

Анализируя содержание Банка данных угроз безопасности информации ФСТЭК России, можно выделить не менее 93 угроз, прямо или косвенно связанных с намеренным вмешательством поставщика услуг (подрядчика, инсайдера), программными закладками, «логическими бомбами» и недеklarированными возможностями. В качестве гипотезы, нуждающейся в тщательной проверке, обозначим идентификаторы УБИ этих угроз: 1, 3, 5 — 8, 10, 12, 14 — 17, 20 — 22, 24, 25, 27 — 32, 34, 35, 37, 39 — 41, 43 — 45, 48, 51, 54, 55, 57 — 60, 62, 64 — 66, 68, 70, 72 — 77, 79 — 81, 83, 84, 86 — 92, 96, 97, 100, 101, 107 — 109, 111 — 113, 115, 117, 119, 120, 134 — 138, 141 — 143, 145, 147, 149, 150, 153, 154, 164, 171. Объекты воздействия данных угроз разнородны и включают программное и аппаратное обеспечение СВТ, облачные

сервисы и виртуальные машины. Условия для реализации угроз и возможный потенциал нарушителя также различаются в соответствии со спецификой конкретной угрозы.[2] Однако в условиях преобладания иностранных программно-аппаратных средств общим становится возможное злонамеренное участие представителей иностранных государств в формировании благоприятных условий для реализации данных угроз.

Объекты воздействия данных угроз можно классифицировать по признаку собственности:

- информационные системы органов государственной власти и государственных предприятий;
- информационные системы коммерческих предприятий;
- персональные ЭВМ, принадлежащие физическим лицам.

При этом, в условиях обострения внешнеполитической обстановки, можно предполагать несколько сценариев, направленных на дестабилизацию единого информационного пространства, формируемого отечественными информационными системами.

Сценарий 1 — экономическая изоляция в области информационных технологий. Воздействие осуществляется целиком на отрасль информационных технологий. В качестве возможных мер воздействия: запрет на продажу российским юридическим лицам программного и аппаратного обеспечения, производимого в странах-участницах ограничительной политики в отношении России; ограничения на продажу российским физическим лицам программного и аппаратного обеспечения. В качестве дополнительной меры давления можно рассматривать возможное прекращение поддержки российских пользователей. В данной ситуации достижимы последствия:

- невозможность поддержки доверенной вычислительной базы информационных систем за счёт отсутствия возможности обновления ключевых компонентов, содержащих уязвимости;
- при долгосрочном воздействии — разрушение информационной инфраструктуры за счёт естественного старения и выхода из строя аппаратного