УДК 004.056

ОБЗОР СУЩЕСТВУЮЩИХ ПОДХОДОВ ПО ПРЕДОТВРАЩЕНИЮ ИНСАЙДЕРСКИХ УГРОЗ В РОССИЙСКИХ ОРГАНИЗАЦИЯХ ПО РАЗРАБОТКЕ ПО

Озолиньш М.П.[1]

Научный руководитель – доктор технических наук, профессор практики Лившиц И.И.[1]

[1]Университет ИТМО

marijaozolinsh@gmail.com

Введение

Ежегодно в исследованиях по киберугрозам в Российской Федерации в топе самых актуальных угроз находятся инсайдерские (внутренние) угрозы [1]. Ухудшает обстановку высокие темпы цифровизации и импортозамещения из-за геополитической обстановки. Увеличивается рост компаний по разработке ПО, но из-за скорости перехода не всегда удается следовать всем стандартам безопасной разработки и организации ИБ в компании. Вышеперечисленные факторы в аналитической статье от Positive Technologies [2] являются основным бустером для кибератак в РФ, а социальная инженерия – одним из превалирующим методом. Следовательно, психологическое давление на внутренних сотрудников будет высоким, а если не выявить внутреннего нарушителя, то потери будут колоссальными. Однако лишь незначительный процент организаций способный раскрыть внутренние инциденты ИБ [3]. Целью обзора является аналитическое сравнение подходов по предотвращению инсайдерских угроз, а в дальнейшем планируется создание методологии для уменьшения данного риска.

Основная часть

В рамках обзора реализованы следующие задачи:

1. Обзор правовых, организационных и технических мер по предотвращению инсайдерских (внутренних) угроз;
2. Аналитическое сравнение мер. В результате которого выявлены косвенные факторы, которые не учтены в существующих практиках по организации ИБ в РФ;
3. Создана тестовая версия методологии, учитывающая выявленные факторы. В дальнейшем планируется внедрение методологии в организацию и тестирование ее эффективности.

Выводы

В результате обзора выявлены факторы, приводящие к инсайдерским рискам, но ранее они не были комплексно рассмотрены в рамках обеспечения безопасности организации. Создана тестовая методология, которая в дальнейшем будет реализована.

Литература

1. Дайджест и обзоры: Офицеры безопасности опасаются утечек данных из-за ошибок [Электронный ресурс]. - Режим доступа: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/ofitsery-bezopasnosti-opasayutsya-utechek-dannykh-iz-za-oshibok (Дата обращения 18.02.2026).
2. CODE RED 2026: Актуальные киберугрозы для российских организаций [Электронный ресурс]. - Режим доступа: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (Дата обращения 18.02.2026).
3. Дайджест и обзоры: Лишь 23% организаций способны раскрыть внутренние инциденты ИБ [Электронный ресурс]. - Режим доступа:

https://www.infowatch.ru/analytics/daydzhesty-i-obzory/lish-dvadtsat-tri-protsentov-organizatsiy-sposobny-raskryt-vnutrenniye-intsidenty-ib (Дата обращения 18.02.2026).