Секция «10.5 Компьютерное право и информационная безопасность»

Правовые, организационные и технические аспекты информационной безопасности при работе с подрядчиками

Научный руководитель – Чимитдоржиев Нимбу Баирович

Елатников Никита Васильевич
Студент (специалист)
Национальный исследовательский университет «Высшая школа экономики»,
Московский институт электроники и математики им. А.Н. Тихонова, Москва, Россия
E-mail: q33rtty@yandex.ru

Повсеместная цифровизация деятельности предприятий, организаций в различных отраслях экономики, государственных органов, организаций и учреждений приводит к положительным эффектам в виде оптимизации времени и ресурсов, повышению производительности производства, удобству при оказании различного рода услуг населению. Однако с ростом использования цифровых технологий растет и ландшафт киберугроз, увеличение масштаба последствий от реализованных киберинцидентов. Ущерб от кибератак и киберпреступности за 2025 год в России оценивается в 1,5 трлн руб. [1] и прогнозы показывают, что количество и качество кибератак будут только расти.

Одной из критичных киберугроз сегодня считается угроза цепочки поставок. И речь здесь не только про намеренные или случайно оставленные уязвимости в разрабатываемом и поставляемом по заказу программном обеспечении (далее - ПО) или других продуктах, связанных с цифровыми технологиями. Такое ПО сегодня, по крайней мере для объектов критической информационной инфраструктуры, требует прохождения оценки на безопасность, наличия в реестре отечественного ПО. При жестком выполнении предъявляемых требований риски совершения компьютерных атак, использующих уязвимости и/или ошибки конфигурации в программном обеспечении, значительно снижаются.

Проблема, которую часто игнорируют организации, предприятия, госорганы, заключается в неконтролируемом доступе к их информационной инфраструктуре, критическим информационным ресурсам, системам, третьих лиц – подрядчиков, осуществляющих работы или оказывающих услуги по обслуживанию, поддержке таких систем, не смотря на наличие договоров (контрактов), заключенных на законном основании.

Первый аспект – правовой. Проблема заключается в нередком отсутствии в договорах на работы третьих лиц обязанности по обеспечению информационной безопасности и, даже, обязательств по неразглашению конфиденциальной информации.

Второй аспект – организационный. Проблема заключается в том, что в иногда договорах не предусмотрена процедура контроля за действиями работников подрядчиков, недостаточно точно прописаны действия, которые сторонний специалист может проводить на объекте работ (в информационной системе) и время проведения работ.

Третий аспект – технический. Проблема заключается в отсутствии или недостаточности описания технических мер защиты информации при проведении работ не только удаленным способом, но и очно – отсутствуют базовые требования ИБ к применяемым техническим средствам сторонних работников, не предусмотрены технические средства на стороне заказчика работ, позволяющие как минимум контролировать действия в системе.

В настоящее время в нормативные документы по ИБ включаются требования по обеспечению ИБ при работе подрядчиков в государственных информационных системах [2], а ФСБ России, например, при обеспечении функционирования ГосСОПКА информирует [3] субъектов КИИ через НКЦКИ о необходимости обеспечения безопасности при совершении подрядчиками удаленного доступа для проведения соответствующих работ. Используя

эти рекомендации и требования будет целесообразным выделить базовые (универсальные) рекомендации во всех трех аспектах, которые могут являться основой для решения указанных выше проблем во всех трех аспектах – правовом, организационном и техническом.

Источники и литература

1) Ведомости: https://www.vedomosti.ru/technologies/trendsrub/articles/2025/12/08/1160280-volnoi-kiberatak
2) ФСТЭК России: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117
3) Безопасность пользователей в сети интернет: https://safe-surf.ru/upload/ALRT/ALRT-20250222.1.pdf