Щит против киберугрозы

БЕЗОПАСНОСТЬ **«Транснефть» совершенствует систему информационной безопасности и защиты автоматизированных систем. Если раньше киберугрозы были фантастикой, то сегодня стали повседневностью, на которую необходимо оперативно реагировать.**

Текст: Вадим Оноприюк, Анна Полякова
Фото: Руслан Шамуков

В Москве состоялся Экспертный совет ПАО «Транснефть». В этот раз экспертному сообществу предложили обсудить тему противодействия киберугрозам при обеспечении безопасности объектов критической информационной инфраструктуры. Состав участников (представители министерств и ведомств, силовых структур, Госдумы, Совета Федерации, а также юристы и бизнесмены) и их живой интерес подчеркнули актуальность темы.

За четыре года в условном рейтинге бизнес-рисков киберугрозы поднялись с тринадцатого на третье место.

И все чаще отмечается растущая скоординированность действий киберпреступников. При этом методы, способы и средства совершения компьютерных преступлений становятся все изощреннее. Если раньше целями атак был вандализм – заражение вирусом, удаление важной информации, кража и дальнейшая публикация конфиденциальных сведений, то сейчас это извлечение финансовой выгоды, промышленный шпионаж, реализация конкурентной борьбы, дезорганизация производственных процессов, решение политических задач путем взлома сетей или отдельных компьютеров. Нельзя отрицать и существование киберугроз со стороны террористических организаций.

10
МЕСТО ЗАНИМАЕТ РОССИЯ ПО ИНДЕКСУ КИБЕРБЕЗОПАСНОСТИ МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ (1 – СИНГАПУР, 2 - США, 3 - МАЛАЙЗИЯ, ..., 24 – ГЕРМАНИЯ, 32 – КИТАЙ)

НАЙТИ И ОБЕЗВРЕДИТЬ

Производственный процесс транспортировки нефти и нефтепродуктов автоматизирован, и это в значительной степени упрощает производство, но проявляются возможности незаконного проникновения в программное обеспечение.

– «Транснефть» автоматизировала практически все технологические процессы начиная от складского учета и делопроизводства и заканчивая диспетчеризацией и регулированием грузопотоков, – сказал президент компании Николай Токарев. – Мы практически ежедневно сталкиваемся с большим количеством кибератак. Это вызывает серьезную озабоченность, и стало чувствительной для нас темой. Невозможно представить, что это сможет повлиять, тем или иным способом вмешаться в деятельность «Транснефти» и надолго нарушить ее рабочий график.

В последние годы появился новый вид вредоносных программ, которые способны заразить целый ряд моделей устройств крупнейших производителей автоматизированных систем управления технологическими процессами (АСУТП) и систем диспетчерского управления. Для предприятий «Транснефти», эксплуатирующих аналогичное оборудование, этот вид вредоносного ПО особенно опасен: его активность может нанести вред производственному процессу. В компании и дочерних обществах эксплуатируется более пяти тысяч АСУТП и более сотни информационных систем.

– Ресурсы компании подвергаются нарастающему числу атак, – сказал вице-президент ПАО «Транснефть» Владимир Рушайло. – Только за три квартала 2017 года по сравнению с аналогичным периодом прошлого года число электронных писем с нежелательным содержимым, с помощью которого в корпоративные сети могут внедряться различные вредоносные программы, увеличилось на 60% и достигло в абсолютном исчислении около 10 млн.

СИСТЕМНЫЙ ПОДХОД

Противодействие киберугрозам организовано в компании на системной основе. В связи с утверждением новой Доктрины информационной безопасности РФ, изменением федерального законодательства в июле в компании введена в действие новая редакция Политики информационной безопасности ПАО «Транснефть». Разработана Программа противодействия киберугрозам информационно-технологическим ресурсам ПАО «Транснефть». Она определила способы и меры противодействия угрозам информационной безопасности и непрерывности функционирования объектов. Этот же документ регламентирует организацию планирования и применения мер по минимизации последствий кибернесягательств.

В компании формируется Центр компьютерной безопасности. Его работа будет осуществляться во взаимодействии с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Талия Хабриева,
директор Института законодательства и сравнительного правоведения при Правительстве РФ, академик РАН

Требования к объектам критической информационной инфраструктуры – сложные и постоянно обновляются. Правовое регулирование еще не завершено. Новизна закона состоит в том, что компания сама категорирует объекты. Это создает определенную свободу, но с другой стороны – налагает обязанности. Дает больше возможностей компании к принятию локальных актов. Это соответствует мировым трендам. Мы не знаем, какие информационные технологии появятся завтра. Именно сама компания может определить, что можно сделать, не дожидаясь регулирования более высокого юридического уровня.

ВЫЗОВЫ НОВОГО ВРЕМЕНИ

Тему санкционной политики в отношении крупных российских компаний затронул первый вице-президент ПАО «Транснефть» Максим Гришанин.

– Санкции не оказали заметного влияния на производственную деятельность трубопроводного транспорта страны, так как «Транснефтью» уже достаточно давно реализуется техническая политика замещения импортных материалов и оборудования продукцией отечественного производства, – отметил он. – Однако в 2016 году компания столкнулась с невозможностью продления лицензий и услуг технической поддержки на средство защиты информации, разработанное иностранной компанией. Это лишний раз говорит о том, что при наличии эквивалентных отечественных разработок предпочтение должно отдаваться российским решениям.

По словам первого вице-президента, создание систем защиты информационной инфраструктуры на базе только российских решений пока затруднительно. Некоторые отечественные продукты являются откровенно сырыми. Поэтому пока при использовании российских средств защиты информации приходится дополнять их иностранными системами, что приводит к удорожанию решений.

Как отметил руководитель направления перспективных технологий и защиты критических инфраструктур «Лаборатории Касперского» Георгий Шебулдаев, безопасность информации в офисных системах – это прежде всего защита конфиденциальных сведений.

– Другой фокус в промышленных системах – здесь во главе угла непрерывность технологических процессов, – считает он. – Мы разработали специализированные продукты для применения в промышленных средах. Это защита серверов и средства обнаружения вторжений с учетом специфики технологических протоколов и типовой архитектуры построения промышленной среды. Эти продукты проходят различные испытания в ПАО «Транснефть». Компания – очень требовательный заказчик, и мы рады, что доказали полезность и работоспособность наших решений на реальной инфраструктуре.

По итогам заседания участники отметили, что кибербезопасность является неотъемлемой частью формирующейся в России цифровой экономики, и подчеркнули необходимость совершенствования законов и технологий, особо отметив необходимость перехода на ПО отечественного производства. ■