УДК 343. 73

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ЗА СОСТОЯНИЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПОДРАЗДЕЛЕНИЯМИ ГОСУДАРСТВЕННОЙ СЛУЖБЫ СПЕЦИАЛЬНОЙ СВЯЗИ УКРАИНЫ (ПО МАТЕРИАЛАМ ДНЕПРОПЕТРОВСКОЙ ОБЛАСТИ)

Евгений КУТНИЙ,
заместитель начальника Управления режима и технической защиты информации
Главного управления Национальной полиции в Днепропетровской области,
преподаватель кафедры оперативно-розыскной деятельности
Днепропетровского государственного университета внутренних дел

АННОТАЦИЯ

В статье исследуются особенности осуществления контроля за состоянием технической защиты информации подразделениями Государственной службы специальной связи Украины. Анализ и рекомендации производились на основе материалов указанной выше службы в Днепропетровской области. Акцентируется внимание на том, что одним из основных направлений государственной политики по вопросам обеспечения национальной безопасности в информационной сфере является обеспечение информационного суверенитета Украины.

Ключевые слова: Государственная служба специальной связи и защиты информации Украины, национальная безопасность, информационная сфера, автоматизированные системы класса 1, комплексная система защиты информации.

FEATURES OF MONITORING THE STATE OF TECHNICAL PROTECTION OF INFORMATION BY DIVISIONS OF THE STATE SERVICE OF SPECIAL COMMUNICATION OF UKRAINE (FOR THE MATERIALS OF THE DNIPROPETROVSK REGION)

Evgeny KUTNIY,
Deputy Head of the Regime and Technical Protection of Information Directorate
of the Main Directorate of the National Police in the Dnipropetrovsk Region,
Lecturer of the Department of Operational Investigation Activities
of the Dnipropetrovsk State University of Internal Affairs

SUMMARY

The article explores the features of monitoring the state of technical protection of information by units of the State Service for Special Communications of Ukraine. Analysis and recommendations were made on the basis of the materials of the above service in the Dnipropetrovsk region. It focuses on the fact that one of the main directions of state policy on ensuring national security in the information sphere is ensuring the information sovereignty of Ukraine.

Key words: State Service for Special Communications and Information Protection of Ukraine, national security, information sphere, class 1 automated systems, integrated information protection system.

Постановка проблемы. Согласно Закону Украины «Об основах национальной безопасности Украины» одним из основных направлений государственной политики по вопросам обеспечения национальной безопасности в информационной сфере является обеспечение информационного суверенитета Украины; совершенствование государственного регулирования развития информационной сферы путём создания нормативно-правовых актов и экономических предпосылок для развития национальной информационной инфраструктуры и ресурсов; внедрение новейших технологий в этой сфере; принятие комплексных мер по защите национального информационного пространства [1].

Актуальность темы исследования подтверждается тем, что современный этап реформ в Украине в условиях социально-экономических, политических сдвигов, поляризации мнений и общественных движений, обновления законодательства обусловливает необходимость особого внимания к проблемам соблюдения режима секретности и технической защиты информации при осуществлении служебной деятельности в государственных органах, органах местного самоуправления, на предприятиях, в учреждениях, организациях. Соблюдение требований закона всеми субъектами, которые наделены правом обрабатывать информацию, составляющую служебную или государственную тайну, позволит обеспечить государственную безопасность [2, с. 485].

Состояние исследования. Научный анализ по вопросам, связанным с определением проблем обеспечения технической защиты информации, сохранение служебной и государственной тайны постоянно находятся в поле зрения как отечественных, так и зарубежных учёных. Разные аспекты этой проблемы исследовали такие учёные и практики, как: В.Ю. Артемов, С.Л. Бервенко, А.В. Белий, В.Г. Грищенко, А.Ф. Долженков, В.В. Ефимов, В.П. Захаров, И.М. Зубач, О.В. Кириченко, Д.В. Куценко, В.П. Меживой, В.В. Макаренко, А.И. Марущак,

В.А. Николайчук, О.В. Новиков, А.И. Низельник, В.Д. Пчолкин, С.П. Пекарский, С.А. Панасюк, Э.В. Рыжков, В.А. Черков, М.Ю. Черкова, М.М. Юнаков, А.А. Шлома и др.

Однако указанные вопросы исследованы недостаточно глубоко, подтверждением чему является большое количество нарушений, выявляемых подразделениями Государственной службы специальной связи Украины.

Целью и задачей статьи является освещение особенностей осуществления контроля за состоянием технической защиты информации подразделениями Государственной специальной связи Украины на примере материалов Днепропетровской области.

Изложение основного материала. Обобщение данных по осуществлению контроля за состоянием технической защиты информации должностными лицами Государственной службы специальной связи и защиты информации Украины (Госспецсвязи) на территории Днепропетровской области освещает некоторые позиции [3, с. 3–12].

В течение 2014–2018 годов охвачены проверками: Государственное агентство водных ресурсов Украины; Государственное агентство рыбного хозяйства; Национальное агентство Украины по вопросам государственной службы; Государственное агентство лесных ресурсов Украины; Управления Государственной службы Украины по вопросам безопасности пищевых продуктов и защиты прав потребителей; Государственная аудиторская служба Украины; Государственная казначейская служба; Государственная фискальная служба Украины; Пенсионный фонд Украины; Государственная экологическая инспекция Украины; Государственное агентство автомобильных дорог Украины; Государственная миграционная служба Украины; Антимонопольный комитет Украины; Министерство юстиции Украины; Министерство образования и науки Украины; органы местного самоуправления (городские советы, областные государственные администрации), судебная власть Украины; Управление Службы безопасности Украины в Днепропетровской области; Национальная полиция Украины; Национальная гвардия Украины; Вооружённые силы Украины.

Примерное количество мероприятий государственного контроля в пределах региона составляет 13–17 в течение календарного года, с учётом плановых комплексных, целевых и контрольных проверок состояния технической защиты информации.

Наибольшее количество нарушений характерно для органов государственной власти и организаций, не имеющих штатных подразделений технической защиты информации. В 73% по результатам проведения мероприятий государственного контроля устанавливался факт наличия нарушений норм и требований по технической защите информации 1 категории по отношению к информации, составляющей государственные информационные ресурсы и персональные данные. Указанное состояние характерно для тех субъектов контроля, которые имеют в пределах региона и страны в целом вычислительные сети, не используют для защищённого обмена информацией средства технической и (или) криптографической защиты информации, имеющие действующие экспертные выводы, полученные по результатам государственной экспертизы в сфере технической (криптографической) защиты информации, не пользуются защищенными узлами доступа к сети Интернет.

Процент нарушений норм и требований технической защиты информации 2 категории составляет примерно 67. Указанное состояние характерно для субъектов технической защиты информации, имеющих локальные вычислительные сети (или отдельные электронно-вычислительные машины), расположенные в пределах контролируемой зоны, и осуществляют их эксплуатацию к созданию комплексных систем защиты информации с подтверждённым соответствием. Наиболее характерным указанное является также в отношении государственных информационных ресурсов и персональных данных.

Определённый процент данных нарушений составляют факты осуществления обработки служебной информации в составе автоматизированных систем класса 1 при отсутствии внедрённой комплексной системы защиты информации с подтверждением соответствия. В то же время за последний год количество таких нарушений становится меньше из-за внедрения механизма прохождения государственной экспертизы путём анализа деклараций о соответствии комплексных систем защиты информации требованиям нормативных документов по технической защите информации.

Около 53% субъектов технической защиты информации не выполняют требования антивирусной защиты информации – используются антивирусные продукты, не имеющие действующих экспертных заключений, и (или) обновления антивирусных баз данных осуществляется в нарушение установленного законодательством порядка.

Почти 83% субъектов технической защиты информации продолжают использование с целью обеспечения служебной деятельности программных продуктов, подпадающих под действие персональных специальных экономических и других ограничительных мер (санкций). Указанное наиболее характерно в отношении программного обеспечения финансового учёта и отчётности, антивирусного программного обеспечения.

Нарушение требований технической защиты секретной информации являются редкостью и наиболее характерны для субъектов режимно-секретной деятельности, имеющих значительный документооборот, они используют технические средства обработки секретной информации (как правило, автоматизированные системы класса 1).

Подавляющее большинство выявленных недостатков подпадают под классификацию нарушений 2 категории (создание предпосылок к нарушению конфиденциальности, целостности, доступности, утечки информации по техническим каналам) и случаются вследствие: несвоевременного проведения инструментального контроля защищённости секретной информации; несвоевременного проведения аттестационных работ комплексов технической защиты информации; изменение состава основных технических средств без проведения внеочередных аттестационных работ; нарушение требований предписаний на эксплуатацию.

Единичны случаи нарушения установленного порядка разграничения

доступа и политики безопасности. Основной причиной имеющихся нарушений являются: недостаточное внимание со стороны руководства субъектов технической защиты информации по обеспечению технической защиты информации, отсутствие штатных специалистов или подразделений по технической защите информации, отсутствие или недостаточность финансирования работ по технической защите информации.

По фактам наличия нарушений норм и требований по технической защите информации, подпадающих под классификацию 1 категории, субъектам технической защиты информации даются рекомендации рассмотреть вопрос о приостановлении информационной деятельности на объектах информационной деятельности (объектах электронно-вычислительной техники) до момента создания комплексных систем защиты информации и проведения их государственной экспертизы.

В 75% случаев по результатам проведённых мероприятий государственного контроля с целью выяснения обстоятельств, которые привели к нарушению норм и требований технической защиты информации, анализа возможности утечки информации, определения лиц, совершивших нарушения, было назначено проведение служебных расследований.

По применению мер административного воздействия необходимо отметить, что ответственность, предусмотренная частью 1 статьи 188-31 Кодекса Украины об административных правонарушениях, применяется по результатам проведения контрольных проверок состояния технической защиты информации в случае выявления фактов невыполнения законных требований должностных лиц госслужбы специальной связи и защиты информации Украины по устранению нарушений технической защиты информации.

В 2018 году это примерно 30% от общего количества проведённых мероприятий государственного контроля. К ответственности привлекаются руководители субъектов технической защиты информации или лица, определённые ответственными за непосредственную реализацию мероприятий технической защиты информации.

Ответственность, предусмотренная пунктом 9 части 1 статьи 212-2 Кодекса Украины об административных правонарушениях, применяется в случае выявления нарушений норм и требований технической защиты секретной информации, в результате которых возникает реальная угроза нарушения её конфиденциальности, целостности и доступности. Данные нарушения чаще всего были обнаружены в военных формированиях Вооружённых сил Украины.

Выводы. Следует отметить, что указанные меры контроля технической защиты информации за данный период показывают свою исключительную практичность и целесообразность, что приводит к надлежащему обеспечению режима секретности и охраны государственной тайны в Днепропетровской области. Вопросы деятельности Государственной службы специальной связи и защиты информации Украины, подчинённых режимно-секретных органов и состояние режимно-секретного обеспечения служебной деятельности в государственных органах и подразделениях области находятся под постоянным контролем руководства Управления Государственной службы специальной связи и защиты информации Украины в Днепропетровской области.

Список использованной литературы:

1. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. *Відомості Верховної Ради України.* 2003. № 39.

2. Нізельник О.І., Єфімов В.В. Місце та значення забезпечення державної таємниці в оперативно-розшуковій та кримінально-процесуальній діяльності. *Актуальні проблеми правоохоронної діяльності та юридичної науки* : матеріали міжнародної науково-практичної конференції (19–20 вересня 2013 року, ДДУВС, м. Дніпропетровськ). С. 484–486.

3. Аналітична довідка Управління Державної служби спеціального зв'язку та захисту інформації України в Дніпропетровській області за 2014–2018 роки. Дніпро, 2019. 39 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Кутний Евгений Анатольевич – заместитель начальника Управления режима и технической защиты информации Главного управления Национальной полиции в Днепропетровской области, преподаватель кафедры оперативно-розыскной деятельности Днепропетровского государственного университета внутренних дел

INFORMATION ABOUT THE AUTHOR

Kutniy Evgeny Anatolyevich – Deputy Head of the Regime and Technical Protection of Information Directorate of the Main Directorate of the National Police in the Dnipropetrovsk Region, Lecturer of the Department of Operational Investigation Activities of the Dnipropetrovsk State University of Internal Affairs

efimov2009@i.ua