УДК 004.056

В. В. Єльченков

О. Г. Смирнов

СУЧАСНІ ПІДХОДИ ДО КЛАСИФІКАЦІЇ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ, ЯКА ЦИРКУЛЮЄ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Класифіковано порушення властивостей інформації, які можуть бути реалізовані з боку порушника стосовно об'єкта інформаційної діяльності Національної гвардії України.

Проведено аналіз і класифікацію загроз безпеці інформації на об'єкти інформаційної діяльності та її циркуляції в інформаційно-телекомунікаційних системах, що дозволить спростити процес складання плану захисту інформації та підвищити ефективність його складання на об'єкті інформаційної діяльності та в інформаційно-телекомунікаційній системі.

Запропоновано загальний опис загроз порушення властивостей інформації.

Ключові слова: *комплексна система захисту інформації, спостережність, керованість, технічний захист інформації, загрози безпеці інформації.*

Постановка проблеми. Важливою проблемою Національної безпеки України є забезпечення технічного захисту інформаційних ресурсів сил охорони правопорядку (СОПр).

Вимоги до новітніх засобів оброблення інформації з кожним роком підвищуються. Сьогодні вони здатні передавати величезну кількість інформації на великі відстані, межі яких визначаються тільки особливостями поширення електромагнітних хвиль, саме вони у наш час є основним середовищем передачі інформації, який використовується СОПр для обміну інформацією.

Зазначене вище формує низку завдань, основними з яких є:

– розвиток новітніх методів та засобів, за допомогою яких порушник здатний порушити властивості інформації СОПр;

– ускладнення криптографічних засобів;

– удосконалення безпілотних літальних апаратів (БПЛА) як засобів незаконного порушення властивостей інформації.

Прогрес у різних галузях науки і техніки зумовив створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатися до ліній телекомунікацій та різноманітних технічних засобів, наближатися на певні відстані до джерела інформації з метою порушення її властивостей, пересилання та аналізу розвідувальних даних. Для досягнення цієї мети може використовуватись апаратура радіо, радіотехнічної, оптико-електронної, радіо-теплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок, які можуть бути встановлені на БПЛА.

Захист інформації, що обробляється в інформаційно-телекомунікаційних системах (ІТС), полягає в створенні і підтримці в дієздатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і не технічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації та ІТС у цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і ІТС, що її обробляє. Система зазначених заходів, що забезпечує захист інформації в ІТС, називається комплексною системою захисту інформації (КСЗІ) [3].

Один із важливих організаційних заходів КСЗІ – це план захисту інформації, що є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу ІТС.

План захисту має кілька розділів, одним з яких є складання переліку загроз інформації та опис технічних каналів витоку інформації. Він є результатом комплексного обстеження ІТС. При цьому робота зі складання переліку загроз та опису каналів витоку значно ускладнюється з причини відсутності загального опису загроз безпеці інформації (ЗБІ) та каналів витоку.

На сьогодні особливої актуальності набуває проблема запобігання порушенню властивостей інформації, а саме забезпечення її конфіденційності, цілісності та доступності.

Аналіз останніх досліджень і публікацій. Останнім часом питанню складання переліку загроз з визначенням їх спрямованості приділяється значна увага.

Так, у праці [1] пропонується складати перелік загроз відносно їх впливу на конфіденційність, доступність та цілісність інформації. Недоліком цього підходу є те, що він не враховує вплив ЗБІ на зміну властивостей ІТС, а саме на спостережність та керованість.

У підручнику [2] розроблено перелік ЗБІ щодо порушення конфіденційності, цілісності, доступності інформації та спостережності ІТС. Проте не розглядається вплив ЗБІ на цілісність та керованість ІТС.

Метою статті є удосконалення проведення класифікації загроз порушення властивостей інформації з боку порушника в ІТС СОПр, ураховуючи мініатюризацію засобів технічної розвідки та їх розміщення на БПЛА.

Вдосконалена класифікація загроз порушення властивостей інформації з боку порушника дозволить спростити процес складання плану захисту інформації, врахувати дієві заходи щодо збереження властивостей інформації і, як наслідок, буде сприяти підвищенню ефективності створення і функціонування КСЗІ в ІТС.

Виклад основного матеріалу. Технічний канал витоку інформації (ТКВІ) – це сукупність небезпечних фізичних сигналів, середовища їх поширення та зберігання, об'єкта технічної розвідки й способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об'єкта, який охороняється. Об'єктами захисту від технічної розвідки в ІТС є інформація, що обробляється, та програмне забезпечення, яке призначено для оброблення цієї інформації.

На об'єкті інформаційної діяльності створюються за різних обставин природні канали витоку інформації, що потребують надійного захисту.

Штучні канали витоку інформації створюються навмисно із застосуванням активних способів ведення розвідки за допомогою технічних засобів з метою добування інформації.

У зв'язку з цим особливу роль і місце в діяльності відносно захисту інформації займають заходи щодо створення комплексного захисту інформації (КЗІ).

Технічна розвідка в ІТС ведеться шляхом реалізації загроз. Загрози для інформації, що обробляється в ІТС, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій оброблення та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяють на випадкові та навмисні. Основними видами загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись, є:

– зміна умов фізичного середовища (землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів ІТС;

– наслідки помилок під час проектування та розроблення компонентів ІТС (технічних засобів, технології оброблення інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) ІТС під час експлуатації;

– навмисні дії (спроби) потенційних порушників [8].

Загрози в ІТС можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо - та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації (високочастотне нав'язування);

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку,

маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

З усієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації. Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Реалізація загроз, які призводять до втрати інформацією будь-якої із визначених властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації [3].

Уразливості інформації можуть впливати на неї не безпосередньо, а опосередковано. Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами через неуважність, недбалість, незнання тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи ІТС [окремих компонентів, обладнання, програмного забезпечення (ПЗ) тощо], ініціювання тестуючих або технологічних процесів, які здатні призвести до безповоротних змін у системі (наприклад, форматування носіїв інформації);

– ненавмисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

– помилки під час уведення даних у систему, виведення даних за неправильними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту [4].

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІТС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути [4]:

– порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричних перетворень інформаційних сигналів;

– використання з корисливою метою обслуговуючого персоналу ІТС;

– крадіжки носіїв інформації, виробничих відходів;

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті електронно-обчислювальної машини, зовнішніх накопичувачів;

– одержання атрибутів доступу з подальшим їх використанням для маскування під зареєстрованого користувача ("маскарад");

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіка тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації.

Згідно із Законом України "Про інформацію" визначені основні функції суб'єктів забезпечення національної безпеки України (інформаційна сфера окремо не виділена):

– вироблення і періодичне уточнення стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;

– створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;

– удосконалення її організаційної структури;

– підготовка сил та засобів суб'єктів системи до їх застосування згідно з призначенням;

– постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

– систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;

– прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;

– розроблення науково-обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;

Для кожної із загроз необхідно визначити:

– на порушення яких властивостей інформації або ІТС вона спрямована;

– джерела виникнення;

– можливі способи здійснення загроз [5].

Нормативними документами системи технічного захисту інформації рекомендовано розглядати вплив ЗБІ на такі властивості інформації та ІТС:

– конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

– цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;

– доступність інформації – властивість ресурсу системи (послуги, об'єкта, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

– цілісність ІТС – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

– спостережність ІТС – властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушенню політики безпеки і/або забезпечення відповідальності за певні дії;

– керованість ІТС – властивість системи, що дозволяє належним чином реагувати на команди керування і/або переходити з одного стану в інший без порушення політики безпеки [4].

Висновок

Таким чином, проведений аналіз і класифікація загроз (уразливостей) властивостям інформації та в ІТС дозволить спростити процес складання плану захисту інформації, а отже, буде сприяти підвищенню ефективності створення і функціонування КСЗІ в ІТС.

Колектив авторів вважає доцільним надалі проаналізувати можливості всіх видів БПЛА, які можуть мати засоби технічної розвідки та порушувати властивості інформації, що циркулює на ОІД НГУ.

Перелік джерел посилання

1. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации: в 2 т. / за ред. В. А. Хорошко. Киев : Арин, 2008. 464 с.

2. Бабак В. П. Теоретичні основи захисту інформації : підручник. Київ : Книжкове вид-во НАУ, 2008. 752 с.

3. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки / за ред. проф. В. О. Хорошка. Київ : ДУІКТ, 2008. 186 с.

4. НДТЗІ 1.5-001-2000. Захист інформації. Технічний захист інформації. Радіовиявлювачі. Класифікація. Загальні технічні вимоги.

5. Соколов А. В., Шаньгин В. Ф. Защита информации в распределительных корпоративных сетях и системах. Москва : ДМК Пресс, 2002. 636 с.

6. Конахович Г. Ф. Защита информации в телекоммуникационных системах. Київ : МК-Пресс, 2005. 288 с.

7. Нормативне забезпечення інформаційної безпеки / С. М. Головань та ін. ; за ред. проф. В. О. Хорошка. Київ : ДУІКТ, 2008. 533 с.

9. Антонюк А. О. Основи захисту інформації в автоматизованих системах : навч. посіб. Київ : КМ Академія, 2003. 244 с.

10. Модель технічних розвідок "ТР-2030". Київ : Адміністрація Держспецзв'язку, 2016. Кн. 1–5.

Стаття надійшла до редакції 17.03.2020 р.

УДК 004.056

В. В. Ельченков, А. Г. Смирнов

СОВРЕМЕННЫЕ ПОДХОДЫ К КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНОЙ ГВАРДИИ УКРАИНЫ

Классифицированы нарушения свойств информации, которые могут быть реализованы с помощью нарушителя относительно объекта информационной деятельности Национальной гвардии Украины.

Проведены анализ и классификация угроз безопасности информации на объекты информационной деятельности и ее циркуляции в информационно-телекоммуникационных системах, что позволит упростить процесс составления плана защиты информации и повысить эффективность его составления на объекте информационной деятельности и в информационно-телекоммуникационной системе.

Предложено общее описание угроз нарушения свойств информации.

Ключевые слова: *комплексная система защиты информации, наблюдаемость, управляемость, техническая защита информации, угрозы безопасности информации.*

UDC 004.056

V. Yelchenkov, O. Smyrnov

MODERN APPROACHES TO CLASSIFICATION OF THE SECURITY THREAT OF INFORMATION OF OBJECTS OF INFORMATION ACTIVITIES OF THE NATIONAL GUARD OF UKRAINE

The article provides a classification of violations of the properties of information that can be implemented with the help of an intruder in relation to the object of information activity of NSU. The most appropriate way to classify threats of all existing ones, specified in the article is the classification of threats based on the result of their influence on information, that is, a violation of its confidentiality, integrity, and availability of information. Information is kept confidential if the established rules for acquaintance with it are observed. Information maintains integrity if the established rules for its modification are observed. Information remains accessible if it remains possible to familiarize yourself with it or modify it in accordance with the established rules for a certain (small) period of time. A special place for determining the classification of each of the threats must be investigated, firstly, on the violation of what properties of information or ITS it is aimed at, secondly, the sources of the threat, and thirdly, possible ways to implement threats.

It is known that information vulnerabilities can affect it not directly, but indirectly. Random threats of a subjective nature (actions carried out by staff or users through carelessness, negligence, ignorance, etc., but unintentionally) can be:

– actions leading to the failure of ITS (individual components), the destruction of hardware, software, information resources (equipment, communication channels, deletion of data, programs, etc.)

– unintentional damage to storage media;

– unlawful change of the ITS operating modes (of individual components, equipment, software etc.), initiation of testing or technological processes that can lead to irreversible changes in the system (for example, formatting of storage media);

– unintentional viral infection of software;

– failure to comply with the requirements for organizational measures of protection of administrative documents in force in ITS;

– errors when entering data into the system, outputting data to incorrect addresses of devices, internal and external subscribers, and the like;

– any actions that may lead to the disclosure of confidential information, attributes of access control, loss of attributes, and the like;

– unlawful implementation and use of software prohibited by the security policy (for example, training and game programs, system and application software, etc.)

– the consequences of the incompetent use of protective equipment.

The analysis and classification of threats to information security at an object of information activities and its circulation in ITS will simplify the process of compiling an information protection plan and increase the efficiency of its compilation at the information activity object in the information and telecommunication system.

The article provides a general description of threats to information property violations.

Keywords: *integrated information protection system, observability, controllability, technical information protection, information security threats.*

Єльченков Віктор Володимирович – слухач інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського
https://orcid.org/0000-0002-6042-0029

Смирнов Олексій Григорович – начальник служби технічного захисту інформації Національної академії Національної гвардії України
https://orcid.org/0000-0002-3533-0072