Капицына Мария Александровна
студентка
Зайцева Виктория Александровна
студентка
Михнев Илья Павлович
канд. техн. наук, доцент, доцент,
Заслуженный работник науки и образования
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

DOI 10.21661/r-471462

АВТОМАТИЗИРОВАННАЯ СИСТЕМА РАДИОНУКЛИДНОЙ СПЕКТРОМЕТРИИ: ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация*: в статье представлены исследования средств защиты информации от несанкционированного доступа автоматизированной системы радионуклидной спектрометрии. В результате проведенных исследований получены показатели защищенности системы, которые позволяют рассчитать и оптимизировать вероятность ущерба от несанкционированного доступа с учетом времени эксплуатации и применяемых средств защиты информации.*

Ключевые слова*: несанкционированный доступ, естественные радионуклиды, информационная безопасность, система радионуклидной спектрометрии, угрозы безопасности информации.*

Поскольку дозовые нагрузки облучения населения в помещениях зависят от содержания активности естественных радионуклидов (ЕРН) в строительных материалах, выбора мест застройки и конструкций зданий, возможно, ограничить облучение населения от природных источников излучения путём вмешательства в сложившуюся практику строительства [1; 8]. Для высокой точности оценки

радиационного фона в жилых помещениях требуется автоматизированная система радионуклидной спектрометрии (АСРС), позволяющая измерять удельные активности ЕРН в объектах внешней среды, а также предельно низкие мощности дозы гамма-излучения с разделением вклада в показания приборов, обусловленного космическим и гамма-излучением от строительных материалов [2].

Для определения удельных активностей ЕРН в строительном сырье, материалах, почве, древесине и др. целесообразно использовать ASRS (Automated Systems Radionuclide Spectrometry) автоматизированную систему радионуклидной спектрометрии с интегрированным универсальным спектрометрическим комплексом (УСК «Гамма Плюс Р») на базе сцинтилляционного гамма-спектрометра, с программным обеспечением «Прогресс – 5.1» [2; 6]. АСРС «Гамма Плюс Р» может использоваться для решения широкого спектра задач радиационного контроля от измерений в области сертификации соответствия пищевой продукции, питьевой воды, строительных материалов, продукции лесного хозяйства и др. до мониторинга и задач радиационного контроля на предприятиях ядерного цикла, а также для решения целого ряда исследовательских задач, связанных с измерением радиоактивности. Но этот спектрометрический комплекс не поставляется с защитой программного пакета от вредоносного кода и НСД, что может повлечь за собой сбои в работе ПК и потерю информации при НСД. Обработка спектров, расчет активности и погрешности производится с использованием программного обеспечения [3].

Управление работой амплитудно-цифрового преобразователя (АЦП) осуществляется при помощи специальных программ, входящих в состав программного пакета [2; 3]. Обработку спектров, расчет активности и погрешности производят с использованием программного пакета «Прогресс – 5.1». В настоящее время резко обострились проблемы защиты АСРС и объектов критической информационной инфраструктуры РФ от кибернетического оружия, что позволило сформировать актуальность исследования, которая имеет место в соответствии с основными документами РФ по безопасности – Стратегии национальной безопасности и Доктрины информационной безопасности РФ [4]. По данным Совета

Безопасности РФ, в 2016 году было совершено более 50 миллионов кибератак на российские информационные ресурсы, причем 60% атак велось из-за рубежа [5].

Для обеспечения требуемого уровня защиты информации от несанкционированного доступа при анализе радиационных характеристик помещений спектрометрическим методом, а также проектировании и работе автоматизированных систем радионуклидной спектрометрии, реализуются организационные, технические и организационно-технические меры защиты информации. Организационные меры предназначены для руководящего состава, органов по защите информации, других пользователей и заключаются в организации, упорядочении, контролю деятельности по защите информации в организации. Технические и организационно-технические меры защиты информации предусматривают применение технических средств, которые объединяются в комплексы средств защиты информации (КСЗИ) и являются составной частью АСРС [6]. Степень реализации мер по защите информации оценивается в процессе проектирования и работы АСРС и зависит от оптимального комплектования КСЗИ средствами защиты информации (СЗИ) и эффективностью функционирования КСЗИ в целом [2; 7]. Известно, что на реализацию несанкционированного доступа (НСД) к информации, приводящих к нарушению нормального функционирования автоматизированных систем радионуклидной спектрометрии, конфиденциальности, целостности и доступности информации, нарушитель всегда будет затрачивать время $T_{нсд}$, необходимое для образования канала реализации угрозы безопасности информации, то есть, указанное время характеризует временной интервал:

$$T_{нсд} = \sum_{i=1}^{4} T_i \qquad (1)$$

где T_1 – выявление уязвимостей программного (аппаратного) обеспечения; T_2 – оценка возможности эксплуатации уязвимости с учетом существующей системы защиты информации предполагаемого объекта воздействия (носителя информации); T_3 – выбора способа реализации несанкционированного доступа; T_4 – осуществление НСД.

Исходя из этого, путем увеличения T_i всегда можно было бы управлять защищенностью информации в АСРС. То есть T_i можно было бы принять в качестве критерия для оценки защищенности информации в АСРС. Тогда путем задания при проектировании АСРС порогового значения $T_{доп\ нсд}$ и обеспечив выполнение условия $T_{нсд} \leq T_{доп\ нсд}$, можно было бы реализовать допустимую защиту информации ограниченного доступа в АСРС. Однако, такой подход не будет отражать реальную картину, так как время T_i – это случайная величина, закон распределения которой сложно вычислить, так как он будет меняться в зависимости от возможностей нарушителя. Кроме того, здесь не учитываются основные факторы эксплуатации, такие как: различные угрозы безопасности информации в АСРС, время эксплуатации АСРС, характеристики используемых средств защиты информации (СЗИ), от которых также может зависеть НСД к информации.

Поэтому для повышения объективности контроля своевременности, достоверности, полноты и непрерывности защищенности информации, проектируемых АСРС целесообразно разработать математическую модель вероятности НСД к изменяющейся информации с учетом условий эксплуатации и состава комплекса средств защиты информации (КСЗИ). На базе найденной модели сформулировать качественные и количественные критерии повышения защищенности информации при проектировании и работе АСРС. Таким образом, НСД к информации в АСРС, будет зависеть от применяемых СЗИ, от количества угроз безопасности информации, степени защищенности и времени эксплуатации АСРС. В соответствии с ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» целью защиты информации является предотвращение ущерба обладателю информации в связи с возможным НСД к информации, нарушением нормального функционирования АСРС, хищения, модификации или уничтожения информации [9].

Очевидно максимальный ущерб может быть нанесен тогда, когда информация в АСРС скомпрометирована полностью. Такая ситуация может возникнуть при следующих условиях: либо при захвате АСРС противником, либо при ситуации, когда суммарные информационно-технические атаки противника

позволяют ему обеспечить НСД к защищаемой информации, циркулирующих по всем защищенным каналам АСРС. Если реализована одна УБ, то при моделировании будем считать, что это приводит к минимальному ущербу. Сформулируем задачу и найдем выражение для вероятности НСД к информации, циркулирующей в АСРС. Пусть проектируется АСРС, содержащая k подразделений, в каждом из которых возможна реализация N_i, $i = 1, 2, \ldots k$ угроз безопасности информации. Всего же АСРС содержит S возможных к реализации УБ, причем

$S = N_1 + N_2 + \ldots + N_k = \sum_{i=1}^{k} N_i$, парирование УБ осуществляется СЗИ, включенных в КСЗИ. СЗИ обладают различными функциональными возможностями по обеспечению защиты, в зависимости от характеристик, реализуемым механизмам защиты, техническим требованиям, совместимостью с другими средствами защиты, экономическими и эргономическими характеристиками. Для различения КСЗИ (СЗИ) целесообразно ввести весовые коэффициенты M_i, $i = 1, 2, \ldots k$. Чем выше гриф секретности обрабатываемой информации, жестче требования к защите и выше требования к техническим характеристикам, тем большее значение должно быть присвоено коэффициенту M_i и наоборот. Далее введем следующую оценку защищенности информации, определяемую как вероятность НСД к информации при реализации всех возможных к реализации УБ одновременно. Максимальный ущерб возникает тогда, когда, как было указано выше, при реализации всех возможных к реализации УБ, то есть:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i} \qquad (2)$$

Теоретически в течение времени эксплуатации АСРС таких попыток может быть бесчисленное множество. Количественно оценить число попыток реализации УБ практически невозможно. Однако можно задать априори шаг указанных попыток во времени. При этом интервал времени, в течение которого может осуществляться одна попытка реализации УБ (T_p) может задаваться с учетом реальных условий эксплуатации и социально-политической, военной обстановки.

Например, шаг реализации УБ в мирное время можно приравнять одному месяцу, недели, а во время боевых действий нескольким дням, суткам, часам и т. д. Для заданного значения интервала T_p можно определить количество возможных попыток реализации УБ R за время эксплуатации АСРС объекта T:

$$R = \frac{T}{T_p}, \tag{3}$$

где T – время эксплуатации, а T_p – шаг реализации УБ.

Зная количество попыток можно оценить вероятность НСД к информации при реализации всех или хотя бы одной УБ за время эксплуатации T:

$$P(t) = 1 - (1 - P_k)^R, \tag{4}$$

где значение $P_к$ – это некоторая оценка, которая характеризует вероятность одной успешной попытки реализации УБ, а $t = T$.

Заметим, что ранее нами были приведены два метода расчета оценки $P_к$:P_x и P_y для наилучшего и наихудшего случая соответственно. Следовательно, если необходимо рассчитать вероятность того, что за период времени T будет осуществлен НСД к информации при реализации хотя бы одной УБ, в выражение (4) необходимо подставить значение $P_к = P_x$. С другой стороны необходимо рассчитать вероятность наихудшего для системы случая, то есть НСД при реализации всех возможных УБ АСРС одновременно. Тогда в выражение (4) в качестве $P_к$ необходимо подставить значение P_y [10].

Установлено, что наименьшее значение P_x = 0,23 принимает в АСРС, где весовые коэффициенты КСЗИ по подразделениям имеют наибольшие значения. В других АСРС при меньших весовых коэффициентах КСЗИ величина P_x принимает меньшие значения. Вызывает интерес тот факт, что в случае, когда весовые коэффициенты КСЗИ равномерны во всех подразделениях одной АСРС, вероятность реализации хотя бы одной УБ ниже, чем в другой АСРС с подразделениями, имеющими различные весовые коэффициенты КСЗИ. Причем общий весовой коэффициент КСЗИ всех подразделений обоих АСРС одинаков [10]. Можно сделать вывод, что P_x существенно увеличивается с ростом попыток реализации

УБ. Так для АСРС P_x при одной попытке равна 0,25. При осуществлении нарушителем пяти попыток такая вероятность достигнет значения 0,76 [11]. Таким образом, разработанные аналитические оценки позволяют на этапах проектирования АСРС рассчитать верхнюю и нижнюю границы вероятности НСД к информации, что имеет исключительно важное значение для проектирования АСРС. Так как дает возможность при проектировании оптимизировать вероятность возникновения ущерба относительно времени эксплуатации, количества УБ, применяемых средств защиты информации, заданного грифа секретности информации и количества попыток реализации УБ.

Список литературы

1. Михнев И.П. Информационная безопасность спектрометрических систем при определении радиационных характеристик в помещениях Волгоградской области / И.П. Михнев, Н.А. Сальникова // Известия ВолгГТУ. Серия: Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – №13 (177). – Волгоград, 2015. – С. 109–113.

2. Камаев В.А. Влияние гамма-фона помещений Волгоградской области на индуцирование рака / В.А. Камаев, И.П. Михнев, Н.А. Сальникова // Известия ВолгГТУ. Серия: Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – №14 (178). – Волгоград, 2015. – С. 60–63.

3. Сальникова Н.А. Проведение аттестации знаний студентов с помощью компьютерного тестирования / Н.А. Сальникова, И.П. Михнев // Известия ВолгГТУ: Межвуз. сб. науч. ст. – №7 (33). – Волгоград, 2007. – С. 182–184.

4. Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. №646) // Собрание законодательства РФ. – 12.12.2016. – №50. – Ст. 7074.

5. Совбез: Число кибератак на РФ за 2016 год выросло втрое // Российская газета. – 15.02.2017 [Электронный ресурс]. – Режим доступа: https://rg.ru/2017/02/15/sovbez-chislo-kiberatak-na-rf-za-2016-god-vyroslo-vtroe.html (дата обращения: 07.05.2018).

6. Михнев И.П. Информационная безопасность в современном экономическом образовании. // Международный журнал прикладных и фундаментальных исследований. – 2013. – №4. – С. 111–113.

7. Сидякин П.А. Материалы для снижения гамма-фона и концентрации радона в помещениях / П.А. Сидякин, О.П. Сидельникова, Ю.Д. Козлов [и др.] // Строительные материалы. – 1998. – №8. – С. 26–27.

8. Михнев И.П. Природные радионуклиды как источник фонового облучения населения Нижневолжского региона / И.П. Михнев, С.В. Михнева // Образование и наука: современные тренды: коллективная монография (Чебоксары, 15 март 2018 г.) / Гл. ред. О.Н. Широков – Чебоксары: ЦНС «Интерактив плюс», 2018. – С. 151–166.

9. ГОСТ Р 50922–2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 8 с.

10. Михнев И.П. Положительные и отрицательные стороны мультимедийных технологий. // Роль и место информационных технологий в современной науке: сборник статей Междунар. науч.-практ. конференции (10.04.2018, г. Челябинск). В 2 ч. Ч. 2. – Уфа: АЭТЕРНА, 2018. – С. 56–59.

11. Михнев И.П. Информационная безопасность на просторах мобильного интернета // Образовательные ресурсы и технологии. – 2015. – №4 (12). – С. 66–70.