DOI 10.31483/r-11199

Михнев Илья Павлович

Сальникова Наталия Анатольевна

Мединцева Ирина Петровна

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ РАДИОНУКЛИДНОЙ СПЕКТРОМЕТРИИ НА БАЗЕ СЦИНТИЛЛЯЦИОННОГО ГАММА-СПЕКТРОМЕТРА

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

В монографии представлены исследования средств защиты информации от несанкционированного доступа автоматизированных систем радионуклидной спектрометрии на базе сцинтилляционного гамма-спектрометра. 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. Разработанные аналитические оценки позволяют на этапах проектирования автоматизированных систем рассчитать верхнюю и нижнюю границы вероятности несанкционированного доступа к конфиденциальной информации.

***Keywords**: natural radionuclides, information security, unauthorized access, design of automated systems, system radionuclide spectrometry, threats to information security.*

The monograph presents studies of information protection tools against unauthorized access to automated radionuclide spectrometry systems based on a scintillation gamma spectrometer. As a result of the conducted researches, the system's security

indicators have been obtained, which allow to calculate and optimize the probability of damage from unauthorized access taking into account the operating time and the applied information protection means. The developed analytical estimations allow to calculate the upper and lower bounds of the probability of unauthorized access to confidential information at the design stages of automated systems.

При обработке любой значимой информации при помощи отдельного компьютера, а тем более в сети, возникает вопрос о ее защите от несанкционированного доступа и использования. Наиболее распространенный в компьютерных системах способ защиты – использование паролей – более пригоден для защиты доступа к вычислительным ресурсам, нежели для защиты информации. Это своеобразный экран, отгораживающий законных пользователей системы от посторонних, пройдя сквозь который, квалифицированный пользователь получает доступ практически ко всей информации. В настоящее время исключительно важное значение приобрели вопросы, связанные с защитой конфиденциальной информации от несанкционированного доступа при проектировании автоматизированных систем. В последние годы при строительстве зданий используются самые разнообразные строительные материалы, как отечественного, так и зарубежного производства. 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]. Существующая практика производства строительных материалов складывалась с учётом их стоимости. Поэтому учёт дополнительного критерия – степени радиационного воздействия на население приведёт к определённому повышению стоимости производства строительных материалов. 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», обеспечивающий установление класса материала [3]. 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. Установка может поставляться в различной комплектации в соответствии с требованием заказчика. АСРС «Гамма Плюс Р» состоит из блоков детектирования, защиты от внешнего гамма излучения, электронного устройства и внешнего блока питания. 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 [4]. Обнаружение гамма-излучения основано на регистрации эффектов, возникающих при его взаимодействии с веществом. Гамма – кванты, испускаемые атомными ядрами при радиоактивных превращениях, имеют определенные физические характеристики, которые можно использовать для их регистрации. Измеряя энергию и интенсивность испускаемых гамма – квантов, а также оценивая период полураспада их отдельных моноэнергетических групп, можно идентифицировать радионуклиды в измеряемых счетных образцах и достаточно точно определить их абсолютную активность. С целью преобразования аналогового спектрометрического сигнала, поступающего с выхода детектора, в

цифровой применяют амплитудно-цифровой преобразователь (АЦП). Управление работой АЦП осуществляется при помощи специальных программ, входящих в состав программного пакета [5]. 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 [6]. 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 [7].

При проектировании АСРС в условиях внедрения цифровой экономики и развития глобального информационного пространства накопился ряд противоречий, обуславливающих отсутствием научно-методического аппарата и единой методики оценки защищенности информации при проектировании АСРС [8]. Это обусловлено:

– значительной неопределенностью из-за отсутствия статистических данных о функционировании множества средств защиты информации (СЗИ) в условиях роста угроз безопасности (УБ) информации и информационно-технических атак;

– сложностью учета и формализации многих существенных для количественной оценки защищенности АСРС факторов (например, разнообразием информационных технологий, программного обеспечения, технических средств).

Вместе с тем необходимость количественных оценок защищенности в связи с ростом количества УБ, а также сложности объектов анализа становится весьма актуальной. 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 [9]. 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 [10]. 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 [11].

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 НСД; 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 [12].

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 циркулирующей 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 АСРС.

Известно, что классическая постановка задачи разработки комплекса средств защиты информации для обеспечения максимальной эффективности функционирования АСРС в условиях НСД будет иметь вид:

$$U_\Sigma \to \min,$$
$$C = C_{opt} \qquad (2)$$

где U_Σ – суммарный наносимый ущерб; C – затраты на проектирование комплекса средств защиты информации;

или

$$E_З \to \max,\ \delta_З \to \max,$$
$$C = C_{opt}\, C = C_{opt} \qquad (3)$$

где $E_З$ – эффективность функционирования АСРС; $\delta_З$ – относительная эффективность функционирования АСРС.

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется сложностью математического описания снижения возможного НСД от затрат на проектирование КСЗИ. Если зависимость защищенности от стоимости

средств защиты можно получить, имея технические и стоимостные характеристики доступных на рынке средств защиты, но оценить реальный ущерб от НСД чрезвычайно трудно, так как этот ущерб также зависит от множества факторов, влияющих на вероятность ущерба.

Например, ущерб будет зависеть от: количества подразделений, включенных в АСРС, характеристик СЗИ, количества возможных к реализации УБ в АСРС, квалификации нарушителя и количества попыток реализации УБ, последствий несанкционированного доступа и т. д.

Вместе с тем проектирование КСЗИ для АСРС объектов критической информационной инфраструктуры, связанных, например, с управлением атомными электростанциями, для которых НСД к информационным ресурсам может привести к катастрофическим последствиям, выбор СЗИ осуществляется с наилучшими показателями и поэтому, влиянием стоимости средств защиты на эффективность можно пренебречь, то есть если $C << U$, то:

$$U_{\Sigma} = \frac{U}{f(C)} \tag{4}$$

В этом случае (2) и (3) принимают вид:

$$U_{\Sigma} \to \min,$$
$$C \le C_{доп} \tag{5}$$

или

$$E_{З} \to \max,\ \delta_{З} \to \max,$$
$$C \le C_{доп}\, C \le C_{доп} \tag{6}$$

где $C_{доп}$ – допустимые расходы на защиту.

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 [13].

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. Предположим, что возможный НСД к информации при реализации хотя бы одной УБ происходит с вероятностью P_x, а вероятность НСД к информации при реализации всех УБ P_y.

Напомним, что рассматриваемая АСРС содержит S возможных к реализации УБ. Предположим, что все угрозы являются случайными с равновероятным законом распределения. Тогда, вероятность НСД к информации при реализации одной конкретной УБ без относительного места ее реализации и защищенности КСЗИ от НСД определяется как:

$$P_s = \frac{1}{S} \quad (7)$$

Для того, чтобы учесть уязвимости АСРС подразделения, наличие которых является обязательным условием для образования канала реализации УБ [17], необходимо в (7) ввести весовой коэффициент M_i, учитывающий характеристики использованных СЗИ для данного *i*-го подразделения. Если M_i ввести в знаменатель выражения (7), то полученное выражение будет отражать физику процесса НСД к информации при реализации одной УБ *i*-го подразделения, т.е. получим:

$$P_{iS} = \frac{1}{M_i + S} \quad (8)$$

Действительно, если $M_i = 0$, что соответствует отсутствию защиты, то (8) превращается в (7). А если M_i будет возрастать, то вероятность НСД к информации будет уменьшаться, что правильно отражает физику явления.

Существуют различные методы определения точной количественной оценки M_i, например, при помощи экспертных оценок, описанных и реализованных в работах Т. Саати, М. Эддоуса, Р. Стэнсфилда, О.И. Ларичева, В.Б. Коробова [14; 15]. Общим свойством всех методом является возможность варьировать значения в необходимых для задачи пределах, например, в пределах от 1 до 10 или в пределах больших значений. Такое «взвешивание» СЗИ при помощи коэффициента M_i позволяет правильно отражать качественную картину процесса НСД к информации и, следовательно, позволит пользоваться (8) для выработки качественных рекомендаций.

Напомним, что АСРС произвольного *i*-го подразделения содержит возможных к реализации УБ. Следовательно, для вероятности НСД к информации U_i при реализации хотя бы одной УБ из N_i возможных угроз *i*-го подразделения будет справедливо выражение:

$$U_i = 1 - (1 - P_{iS})^{N_i} \quad (9)$$

Однотипные УБ имеются в *k* подразделениях, где также могут образовывать каналы реализации угроз. Поэтому для вероятности НСД к информации при реализации хотя бы одной УБ, с учетом всех *k* подразделений, будет справедливо выражение, определяемое формулой для расчета полной вероятности событий:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \sum_{i=1}^{k} \frac{N_i}{S} \left[1 - (1 - P_{iS})^{N_i} \right] \quad (10)$$

где значение η_i определяется соотношением $\eta_i = \frac{N_i}{S}$.

Значение P_x обозначает вероятность НСД к информации хотя бы в одном подразделении при реализации хотя бы одной УБ, то есть вероятность НСД к информации при реализации хотя бы одной из S угроз.

В случае, если в подразделениях одинаковое количество возможных к реализации УБ, т.е.

$$N_1 = N_2 = ... = N_k, \; S = N_1 + N_2 + ... + N_k = k \cdot N_i,$$

следовательно

$$\eta_i = \frac{N_i}{S} = \frac{N_i}{k \cdot N_i} = \frac{1}{k},$$

тогда формула (5) принимает следующий вид:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \frac{1}{k} \sum_{i=1}^{k} \left[1 - (1 - P_{iS})^{N_i} \right] \quad (10.1)$$

Заметим, что формула (10 и 10.1) определяет вероятность НСД к информации при реализации хотя бы одной из возможных УБ для всех подразделений в АСРС. Справедливо полагать, что в этом случае общий причиняемый ущерб будет минимально возможным. С другой стороны, вероятность НСД к информации при реализации хотя бы одной УБ как характеристика защищенности будет принимать максимальное возможное значение, т.е. верхнюю граничную оценку вероятности НСД к информации в АСРС.

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:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i} \quad (11)$$

Таким образом, приведены две оценки защищенности АСРС P_x и P_y и дают верхнюю и нижнюю границы вероятности НСД к информации, что соответствует наилучшему и наихудшему случаю причинения ущерба АСРС в целом.

Тем не менее, очевидно, что выражения (10) и (11) справедливы только для одной попытки реализации УБ.

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 [16]. 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 суткам, 24 часам и т. д. Для заданного значения интервала T_p можно определить количество возможных попыток реализации УБ R за время эксплуатации АСРС объекта T:

$$R = \frac{T}{T_p}, \tag{12}$$

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

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

$$P(t) = 1 - (1 - P_k)^R, \tag{13}$$

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 (13) 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 (13) в качестве $P_к$ необходимо подставить значение P_y.

Следует подчеркнуть, что выражение (13) можно использовать как по всему перечню УБ для конкретной АСРС, так и выборочно, для угроз, составляющих определенную направленность. В частности, можно выделить УБ, при реализации которых нарушается конфиденциальность информации, ее целостность или доступность. Для разных АСРС ущерб от реализации УБ различной направленности может существенно отличаться. Это связано с разнообразием АСРС по выполняемым функциям. Например, угрозы конфиденциальности информации для АСРС информационного характера актуальнее чем угрозы, направленные на нарушение доступности информации. С другой стороны для АСРС управления критически важного объекта угрозы нарушения доступности и целостности информации играют главную роль, в связи с возможными последствиями из-за нарушения работоспособности системы. Такой полиморфизм выражения (13) является его важным достоинством, так как нет необходимости корректировки методов расчета оценки защищенности информации в зависимости от состава УБ в АСРС.

Полученные количественные результаты имитационного моделирования можно представить в табличной или графической форме [17]. При этом следует подчеркнуть, что выражение (13) дает верхнюю границу для вероятности НСД к информации в АСРС, то есть для наихудшего случая, что является особенно важным показателем при проектировании АСРС. В табл. 1 показано, как численно различаются оценки защищенности P_x и P_y для АСРС с разными исходными параметрами. В табл. 2 приведены значения вероятности НСД к информации при реализации как минимум одной УБ и для случая реализации всех УБ одновременно с учетом количества попыток реализации УБ для АСРС 4 и АСРС 7 из табл. 1.

Таблица 1

Оценка защищенности информации для автоматизированных систем радионуклидной спектрометрии

	АСРС 1	АСРС 2	АСРС 3	АСРС 4	АСРС 5	АСРС 6	АСРС 7
S	12	15	20	30	40	50	50

K	3	3	3	3	3	4	4
N_1	3	5	5	4	10	10	10
N_2	4	5	6	6	10	10	10
N_3	5	5	7	10	10	10	10
M_1	3	3	9	5	3	6	4
M_2	4	3	3	2	3	6	5
M_3	2	3	6	9	3	6	9
P_1	0,066	0,055	0,037	0,040	0,030	0,021	0,022
P_2	0,063	0,055	0,047	0,045	0,030	0,021	0,023
P_3	0,071	0,055	0,042	0,034	0,030	0,021	0,020
U_1	0,187	0,248	0,172	0,151	0,265	0,197	0,205
U_2	0,227	0,248	0,254	0,243	0,265	0,197	0,209
U_3	0,309	0,248	0,257	0,296	0,265	0,197	0,186
P_x	0,251	0,248	0,232	0,251	0,265	0,197	0,198
P_y	8,41E-15	1,48E-19	1,77E-25	5,37E-29	2,78E-46	3,09E-67	3,28E-67

Таблица 2

Оценка защищенности информации в АСРС в зависимости от количества возможных попыток реализации угроз безопасности

Количество попыток R	АСРС 4		АСРС 7	
	P_x	P_y	P_x	P_y
0,20	0,056	3,29E-34	0,048	6,36E-73
0,25	0,069	8,25E-32	0,059	4,74E-70
0,33	0,092	1,26E-32	0,079	7,58E-69
0,5	0,134	5,48E-30	0,116	4,67E-67
1	0,251	5,37E-29	0,218	3,08E-65
2	0,439	7,29E-27	0,389	2,45E-62
3	0,580	2,64E-25	0,523	6,37E-60
4	0,685	1,25E-24	0,627	4,25E-57
5	0,764	9,83E-21	0,709	7,67E-53
6	0,823	5,37E-20	0,772	2,92E-51

Проанализируем зависимость количественной оценки вероятности НСД к информации при реализации хотя бы одной УБ P_x от параметров эксплуатации АСРС. Так в табл. 1 наибольшее значение P_x = 0,265 принимает в АСРС №5 при количестве УБ S = 40. При меньших значениях S, величина P_x будет уменьшаться: P_x = 0,232 при количестве S = 20 в АСРС №3, P_x = 0,251 при количестве S = 30 в АСРС №4, P_x = 0,251 при количестве S = 12 в АСРС №1, P_x = 0,248 при количестве S = 15 в АСРС №2. Установлено, что наименьшее значение P_x = 0,232

принимает в АСРС №3, где весовые коэффициенты КСЗИ по подразделениям имеют наибольшие значения (9, 3, 6). В других АСРС при меньших весовых коэффициентах КСЗИ величина P_x принимает меньшие значения. Следует заметить, 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. Так в АСРС №6 и АСРС №7 равное количество $S = 50$, одинаковое количество подразделений $K = 4$ и одинаковое распределение УБ между подразделениями – по 10 УБ в каждом K. Однако, весовые коэффициенты КСЗИ по подразделениям различны: АСРС №6 (6,6,6), АСРС №7 (4,5,9). Общий весовой коэффициент в обоих АСРС равен 18. В тоже время, $P_x = 0{,}197$ для автоматизированной системы радионуклидной спектрометрии №6 меньше чем, $P_x = 0{,}198$ для автоматизированной системы радионуклидной спектрометрии №7 [2; 14].

Проанализировав табл. 2, можно сделать вывод, что P_x существенно увеличивается с ростом попыток реализации угроз безопасности. Так для АСРС №4 P_x при одной попытке равна 0,251. При осуществлении нарушителем пяти попыток такая вероятность достигнет значения 0,764. 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 угроз безопасности, применяемых средств защиты информации, заданного грифа секретности информации и количества попыток реализации угроз безопасности.

Список литературы

1. Камаев В.А. Влияние гамма-фона помещений Волгоградской области на индуцирование рака / В.А. Камаев, И.П. Михнев, Н.А. Сальникова // Известия Волгоградского государственного технического университета. Сер. Актуальные

проблемы управления, вычислительной техники и информатики в технических системах. – 2015. – №14 (178). – С. 60–63.

2. Михнев И.П. Информационная безопасность спектрометрических систем при определении радиационных характеристик в помещениях Волгоградской области / И.П. Михнев, Н.А. Сальникова // Известия Волгоградского государственного технического университета. Сер. Актуальные проблемы управления, вычислительной техники и информатики в технических системах. – 2015. – №13 (177). – С. 109–113.

3. Kamaev V.A., Mikhnev I.P., Salnikova N.A. Natural Radionuclides as a Source of Background Irradiation Affecting People Inside Buildings / V.A. Kamaev, I.P. Mikhnev , N.A. Salnikova // Procedia Engineering 2. «2nd International Conference on Industrial Engineering, ICIE 2016» – 2016. – С. 1663–1672. doi: 10.1016/j.proeng.2016.07.148.

4. Сальникова Н.А., Михнев И.П. Проведение аттестации знаний студентов с помощью компьютерного тестирования / Н.А. Сальникова, И.П. Михнев // Известия Волгоградского государственного технического университета. Сер. Новые образовательные системы и технологии обучения в вузе. – 2007. – Т. 4. – №7 (33). – С. 182–184.

5. Михнев И.П. Обучение и контроль знаний студентов с помощью UniTest // Фундаментальные исследования. – 2008. – №1. – С. 94–95.

6. Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. №646) // Собрание законодательства РФ. – 2016. – 12 декабря. – №50. – Ст. 7074.

7. Совбез: Число кибератак на РФ за 2016 год выросло втрое // Российская газета. – 2017. – 15 февраля [Электронный ресурс]. – Режим доступа: https://rg.ru/2017/02/15/sovbez-chislo-kiberatak-na-rf-za-2016-god-vyroslo-vtroe.html (дата обращения: 15.05.2018).

8. Сорокина Н.В. Правовое регулирование и кадровая обеспеченность органов местного самоуправления: исторический аспект и современные основы: Учебное пособие / Н.В. Сорокина, С.В. Михнева. – Волгоград: Волгоградское научное издательство, 2013. – 211 с.

9. Михнев И.П. Информационная безопасность на просторах мобильного Интернета // Вестник Московского университета им. С.Ю. Витте. Сер. Образовательные ресурсы и технологии. – 2015. – №4 (12). – С. 66–70.

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

11. Михнев И.П. Информационная безопасность в Российской Федерации: современность и перспективы развития / И.П. Михнев, С.В. Михнева, Н.А. Сальникова // Образование и наука: современные тренды: Коллективная монография. Сер. Научно-методическая библиотека / Гл. ред. О.Н. Широков. – Чебоксары, 2018. – С. 103–112. doi:10.21661/r-471355

12. Банько Ю.А. Современные компьютерные угрозы: что реально угрожает бизнесу? / Ю.А. Банько, А.М. Кокорева, И.П. Михнев // Приоритетные направления развития образования и науки: Материалы IV Междунар. науч.-практ. конференции / Редкол.: О.Н. Широков [и др.]. – 2017. – С. 169–171.

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

14. Research of Activity of Natural Radionuclides in Construction Raw Materials of the Volgograd Region / I.P. Mikhnev, N.A. Salnikova, M.B. Lempert // Solid State Phenomena. – 2017. – Т. 265. – SSP. – С. 27–32. doi: 10.4028/www.scientific.net/SSP. 265.27

15. Лемперт М.Б. Биологическое воздействие ионизирующих излучений на состояние здоровья населения / М.Б. Лемперт, И.П. Михнев, Н.А. Сальникова //

Экологические и медицинские проблемы городских экосистем и пути их решения: Материалы региональной научно-практической конференции, посвященной Году Экологии в Российской Федерации в 2017 году. – 2017. – С. 159–164.

16. 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. Сер. Научно-методическая библиотека / гл. ред. О.Н. Широков. – Чебоксары, 2018. – С. 151–166. doi:10.21661/r-470002

17. Сидякин П.А. Материалы для снижения гамма-фона и концентрации радона в помещениях / П.А. Сидякин, О.П. Сидельникова, Ю.Д. Козлов, И.П. Михнев, В.Т. Малый. – М.: Строительные материалы, 1998. – №8. – С. 26–27.

Михнев Илья Павлович – канд. техн. наук, доцент, Заслуженный работник науки и образования, доцент кафедры «Информационных систем и математического моделирования» Волгоградского института управления (филиала) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Россия, Волгоград.

Сальникова Наталия Анатольевна – канд. техн. наук, доцент РАН, доцент кафедры «Информационных систем и математического моделирования» Волгоградского института управления (филиала) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Россия, Волгоград.

Мединцева Ирина Петровна – канд. пед. наук, доцент РАН, доцент кафедры «Информационных систем и математического моделирования» Волгоградского института управления (филиала) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Россия, Волгоград.
