К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ВЫБОРОЧНОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Язов Юрий Константинович, *доктор технических наук, профессор, г. Воронеж*
Машин Олег Анатольевич, *г. Воронеж*
Платонов Борис Федорович, *г. Ростов-на-Дону*

Отмечается выборочный характер контроля защищенности информации в компьютерных системах в условиях ограниченного ресурса сил и времени проведения контрольных мероприятий уполномоченными органами исполнительной власти. Показывается, что существующие методы выборочного контроля, применяемые при оценке качества продукции по числу дефектных изделий, не могут быть применены при оценке эффективности выборочного контроля защищенности информации в информационных системах. В статье рассматривается метод выборочного контроля с однократной выборкой, обосновываются показатели оценки эффективности контроля и приводятся аналитические соотношения для их расчета.

Ключевые слова*: защита информации, компьютерная система, контроль защищенности информации, выборка*

TO THE QUESTION OF ASSESSING THE EFFECTIVENESS OF THE SAMPLING DATA PROTECTION IN INFORMATION SYSTEMS FROM UNAUTHORIZED ACCESS

Yury Yazov, *Doctor of Science (Tech), Professor, Voronezh*
Oleg Mashin, *Voronezh*
Boris Platonov , *Rostov-na-Donu*

Marked selective control of information security in computer systems in resource–limited time and effort implementing control measures by the authorized bodies of executive power. It is shown that the existing methods of sampling control used in the evaluation of the quality of products according to the number of defective products cannot be applied when assessing the effectiveness of the sampling control data protection in information systems. In the article is shown the method of sampling control from a single sample, justified indicators for assessing the effectiveness of controls and gives analytical expressions for their calculation.

Keywords*: information security, computer system, control of data protection, sampling*

Сегодня накопился уже определенный практический опыт организации и ведения контроля уполномоченными федеральными органами исполнительной власти. В ходе проведения плановых контрольных мероприятий проверяется соответствие уровня защиты обрабатываемой в информационных системах (ИС) информации, состава, содержания и эффективности предпринимаемых мер такой защиты требованиям нормативных документов. Отсутствие соответствия требованиям документов рассматривается как нарушение безопасности информации в ИС. Вместе с тем, как правило, контроль проводится в директивные, крайне ограниченные сроки. В этих условиях невозможно охватить контролем все элементы ИС и приходится осуществлять выборочный контроль, то есть оценивать защищенность информации в ИС, прежде всего, от угроз несанкционированно-

го доступа по выборочным данным. При планировании выборочного контроля приходится выбирать первоочередные подлежащие контролю объекты в составе ИС. Как правило, сегодня это осуществляется экспертным путем на основе опыта контролеров, что объясняется отсутствием соответствующего методического обеспечения, позволяющего на количественной основе оценивать эффективность выборочного контроля. Кроме того, важным аспектом организации выборочного контроля является оценка эффективности выборочного контроля по результатам его проведения.

Известные методы выборочного контроля (метод однократной выборки, метод последовательного анализа и др.), используемые при оценке качества продукции по числу дефектных изделий в выбранной для проверки партии таких изделий, не могут быть применимы непосредственно к контролю защищенности информации в ИС, поскольку они не учитывают:

распределение требований и нарушений их выполнения по объектам контроля;

уровень опасности выявляемых нарушений и, следовательно, категории нарушений;

распределения вероятностей возникновения различных нарушений на объектах контроля в составе ИС.

Впервые вопросы выборочного контроля защищенности информации в ИС были подняты в [1], однако там не затрагивались вопросы оценки эффективности выборочного контроля. При этом под эффективностью выборочного контроля понимается по аналогии с [2] степень соответствия результатов контроля поставленной цели, то есть мера достижения поставленной цели контроля.

В данной статье рассматривается подход к оценке эффективности выборочного контроля в случае применения методов однократной выборки с учетом категории возможных нарушений требований безопасности информации, а также распределения нарушений по объектам контроля в составе ИС и вероятностного характера их возникновения.

Как правило, на практике целями контроля являются:

выявление всех возможных нарушений требований нормативных документов, которые имеют место в ИС на момент проведения контрольных мероприятий. В этом случае эффективность контроля характеризует степень выявления нарушений, которые имеют место в ИС;

охват всех объектов в составе ИС, на которых обрабатывается защищаемая информация, на предмет выявления нарушений требований по защите информации. В этом случае эффективность контроля характеризует степень охвата контролем объектов, на которых могут быть нарушения безопасности.

Наличие нескольких целей контроля обусловливает возможность применения разных показателей его эффективности. Важным при выборе таких показателей является определение состава элементов ИС, которыми могут быть:

- разработанные документы по защите информации (ЗИ) в ИС на предприятии (в организации), касающиеся классификации ИС по классам защищенности, частной модели угроз безопасности информации, требований по ЗИ для данной ИС, сертификаты применяемых средств защиты, планирующие и отчетные документы, документы по видам обеспечения (финансовому, кадровому, материальному и т.д.) работ по ЗИ в ИС и др.;

- ИС в целом, если требования по защите информации предъявляются к ИС в целом (например, по организации такой защиты);

- программные и программно-аппаратные средства в составе ИС, такие как серверы, рабочие станции, промышленные контроллеры, межсетевые экраны, шлюзы, proxy-серверы, коммутаторы и другие элементы, предназначенные для сбора, обработки, передачи, хранения и распределения защищаемой информации.

При выборе показателей необходимо учитывать следующее:

1. Эффективность функционирования той или иной системы или проведения мероприятий можно оценивать как по «внутренним» (внутрисистемным), так и по «внешним» (внешнесистемным) показателям. При этом внутрисистемными показателями оценивается, как правило, качество выполнения системой своих функций или выполнения намеченной совокупности мероприятий, а внешнесистемными – влияние функционирования системы (проведения мероприятий) на функционирование «надсистемы». В частности, внутренними показателями контроля могли бы быть показатели, оценивающие степень охвата контролем объектов в составе ИС, относительное количество выявляемых нарушений, и т.п., а внешнесистемными – повышение показателя защищенности ИС от угроз безопасности информации в результате проведения контроля. В данной работе рассматриваются только внутрисистемные показатели.

2. Для оценки эффективности выборочного контроля целесообразно применять систему взаимосвязанных показателей, имеющую иерархи-

ческую структуру. При этом на нижних уровнях должны находиться частные показатели, с помощью которых оцениваются отдельные аспекты контроля или отдельные мероприятия по контролю, а также аспекты функционирования элементов ИС, существенные для оценки эффективности выборочного контроля, например, возможность возникновения нарушений на объектах контроля и возможность выявления нарушений в ходе проведения контрольных мероприятий, временные (вероятностно-временные) характеристики проведения контрольных мероприятий на каждом объекте контроля и др.

3. Выборочный контроль по своей природе является случайной процедурой, поскольку не только выбор объектов контроля зачастую является случайным, но и возникновение и выявление нарушений также происходят с некоторой вероятностью. В связи с этим в качестве частных показателей при оценке эффективности выборочного контроля целесообразно использовать вероятностные показатели.

С учетом изложенного для оценки эффективности выборочного контроля могут быть применены показатели, приведенные на рис.1.

Рассмотрим соотношения для расчета показателей для случая, когда эффективность выборочного контроля оценивается по результатам проведения контрольных мероприятий.

Пусть в соответствии с нормативными документами нарушения требований по ЗИ категорированы и в ИС выявлено m_s нарушений S-ой категории.

Показатель эффективности выборочного контроля «степень выявления нарушений определенной категории» - это отношение количества выявленных в ИС нарушений m_s к количеству (M_s) имеющихся в ней нарушений s-ой категории по определению рассчитывается по формуле:

$$\eta_{des} = \frac{m_s}{M_s} . \qquad (1)$$

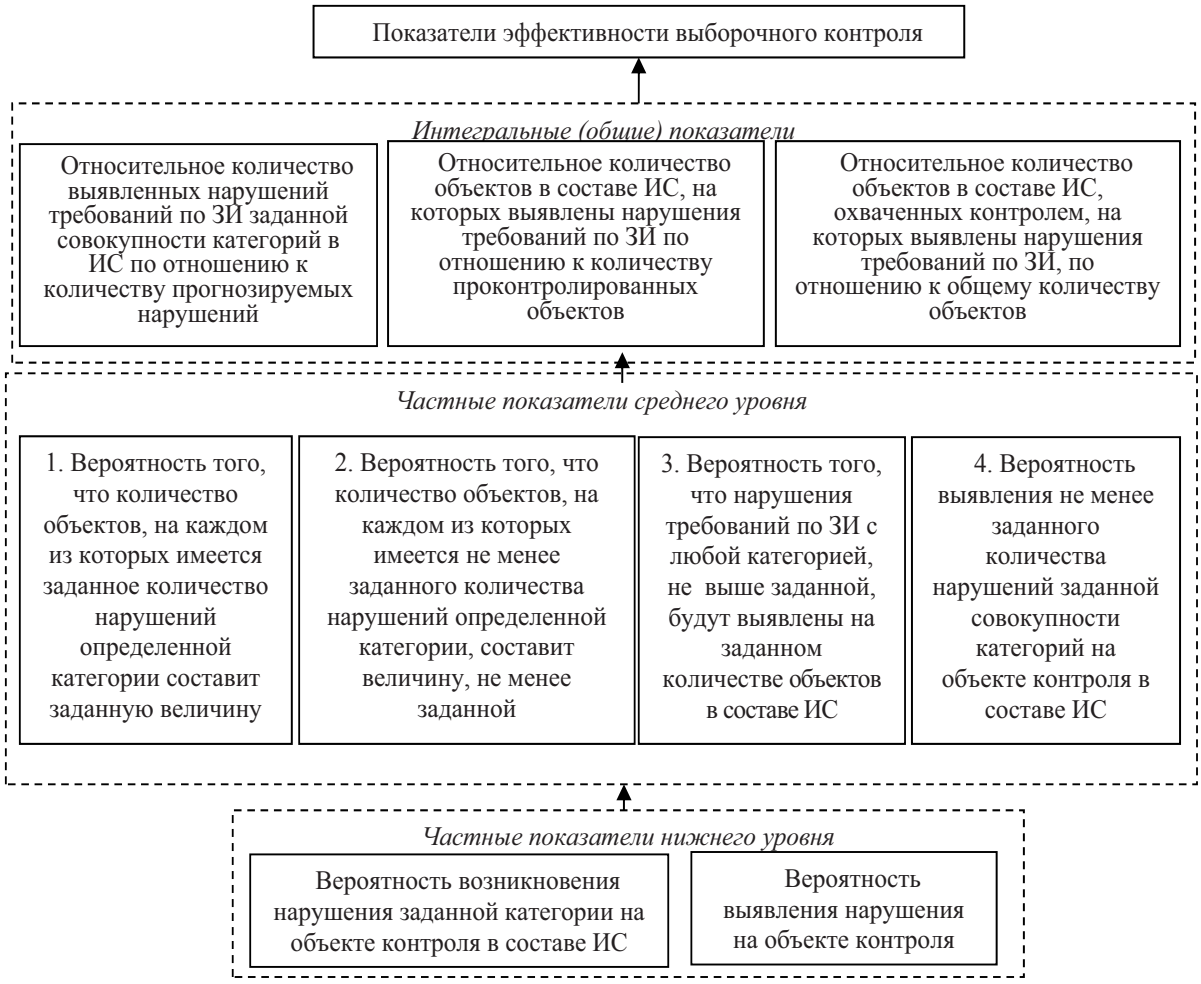

***Рис.1**. Показатели эффективности выборочного контроля защищенности информации в информационных системах*

Если на k-м объекте имеются нарушения разных категорий и необходимо оценить эффективность выборочного контроля применительно ко всем категориям, то используется показатель «степень выявления нарушений безопасности информации», который рассчитывается следующим образом:

$$\eta_{des}(k) = \frac{\sum_{s=1}^{s_{\max}} m_s(k)}{\sum_{s=1}^{s_{\max}} M_s(k)}, \quad (2)$$

где s_{max} - максимальный номер категории нарушений, имеющих место в ИС;

$m_s(k)$, $M_s(k)$ - выявленное и максимально возможное количество нарушений s-й категории на k-м объекте в составе ИС соответственно.

Применительно ко всем объектам в составе ИС, вошедшим в выборку, формула 2 имеет вид:

$$\eta_{des} = \frac{\sum_{k=1}^{n}\sum_{s=1}^{s_{\max}} m_s(k)}{\sum_{k=1}^{n}\sum_{s=1}^{s_{\max}} M_s(k)}, \quad (3)$$

Важная особенность расчета этого показателя по приведенным соотношениям состоит в том, что необходимо знать имеющееся количество нарушений на объектах в ИС. Однако на практике, как правило, это неизвестно. Вместе с тем в этом случае может быть использовано прогнозное значение количества нарушений на основе статистических данных по результатам предыдущих контрольных мероприятий. По таким данным может быть оценена вероятность возникновения нарушения заданной категории s на каждом k-м объекте в составе ИС $P_{gen}(k,s)$. Тогда формула (2) преобразуется к виду:

$$\eta_{des} = \frac{\sum_{s=1}^{s_{\max}} m_s(k)}{\sum_{s=1}^{s_{\max}} P_{gen}(k,s)\cdot M_s(k)}, \quad \sum_{s=1}^{s_{\max}} P_{gen}(k,s) > 0., \quad (4)$$

а для ИС в целом:

$$\eta_{des} = \frac{\sum_{k=1}^{n}\sum_{s=1}^{s_{\max}} m_s(k)}{\sum_{k=1}^{n}\sum_{s=1}^{s_{\max}} P_{gen}(k,s)\cdot M_s(k)}, \quad \sum_{k=1}^{n}\sum_{s=1}^{s_{\max}} P_{gen}(k,s) > 0. \quad (5)$$

Как правило, максимально возможное количество нарушений категории s на каждом n-м объекте соответствует количеству требований по ЗИ, предъявляемых к данному объекту в составе ИС в соответствии с действующими нормативными документами, невыполнение которых приводит к нарушениям s-й категории, и может быть определено на основе анализа этих документов.

Если не учитывать категории нарушений, то соотношения (4) и (5) преобразуются к виду:

$$\eta_{des}(k) = \frac{m(k)}{P_{gen}(k)\cdot M(k)}, \; P_{gen}(k) > 0 \;, \quad (6)$$

$$\eta_{des} = \frac{\sum_{k=1}^{n} m(k)}{\sum_{k=1}^{n} P_{gen}(k)\cdot M(k)}, \quad \sum_{k=1}^{n} P_{gen}(k) > 0\,. \quad (7)$$

Наконец, важными для оценки эффективности выборочного контроля являются показатели, характеризующие охват контролем объектов в составе ИС. К ним относятся два показателя. Первый показатель – это «степень выявления объектов с нарушениями требований по ЗИ информации» определяется как относительное количество объектов (n_{det}) в составе ИС, на которых выявлены нарушения требований по ЗИ, по отношению к количеству проконтролированных объектов n, который рассчитывается при отсутствии категорирования нарушений по определению следующим образом:

$$\eta_{obj} = \frac{n_{\text{det}}}{n}\,. \quad (8)$$

Если категорирование нарушений проводится, то данный показатель может рассчитываться применительно к нарушениям определенной S-й категории:

$$\eta_{obj}^{(s)} = \frac{n_{\text{det}}^{(s)}}{n} \quad (9)$$

или для случая, когда рассматриваются нарушения только с категорией, не менее заданной:

$$\eta_{obj}^{(\geq s_0)} = \frac{n_{\text{det}}^{(\geq s_0)}}{n}\,. \quad (10)$$

Затем данный показатель усредняется с учетом веса каждой категории нарушений:

$$\eta_{obj}(k) = \frac{1}{s_{\max}}\sum_{s=1}^{s_{\max}} \delta_s \cdot \eta_{obj}^{(s)}(k)\,, \quad (11)$$

где $\sum_{s=1}^{s_{\max}} \delta_s = 1$ - для нарушений всех категорий;

$$\eta_{obj}(k) = \frac{1}{\sum_{s=s_0}^{s_{\max}} \delta_s}\sum_{s=s_0}^{s_{\max}} \delta_s \cdot \eta_{obj}^{(s)}(k)\,, \quad (12)$$

где $\sum_{s=1}^{s_{\max}} \delta_s = 1$ - для нарушений с категорией, не менее s_0.

Второй - показатель эффективности выборочного контроля «степень охвата контролем объектов с нарушениями» - относительное количество объектов (n_{det}) в составе ИС, на которых выявлены нарушения требований по ЗИ, по отношению к общему количеству объектов (N) , рассчитывается по аналогичным формулам, только вместо n подставляется величина N .

Полученные соотношения впервые позволяют всесторонне оценить эффективность выборочного контроля безопасности информации в ИС по результатам проведения контрольных мероприятий.

Рассмотрим второй случай, когда оценивается предполагаемая эффективность выборочного контроля применительно к выбранному составу подлежащих контролю объектов без наличия каких-либо приоритетов у объектов контроля. При этом выборочный контроль может быть контролем с однократной выборкой, то есть в течение установленного директивного срока осуществляется одно контрольное мероприятие относительно ИС. Математическая модель оценки эффективности такого статистического выборочного контроля с однократной выборкой сводится к следующему.

Пусть в составе ИС имеется □ объектов, из которых для контроля выбрано *n* объектов. К ним относятся объекты, в которых циркулирует защищаемая информация, то есть должны выполняться требования по ЗИ, соответствующие определенному для данной ИС классу защищенности.

Обозначим через N_ε, $\varepsilon = \overline{1,\mathrm{E}}$, количество объектов в составе ИС, где предположительно имеется хотя бы одно нарушение категории ε , через n_{m_ε} - количество объектов, на которых имеется ровно m_ε нарушений категории ε , а через M_ε - общее количество нарушений требований категории ε , которые могут иметь место в ИС.

При выборочном контроле на некоторых контролируемых объектах n_0 отсутствуют нарушения, а на остальных $n - n_0$ объектах могут иметь место нарушения требований по ЗИ ($n \le N$). Рассмотрим соотношения для расчета первого из частных показателей среднего уровня (см. рис.1) – вероятности $P_{obj}(n_{m_\varepsilon}, n, N)$ того, что количество объектов, на каждом из которых имеется заданное количество нарушений m_ε определенной категории (ε), составит заданную величину n_ε, если контролю подверглись n из N объектов в составе ИС.

Пусть обнаружение нарушений происходит с единичной вероятностью, а сами нарушения достоверно имеют место. Найдем закон распределения числа объектов, на которых имеет место нарушение, в предположении, что нарушения возникают независимо друг от друга и равновероятно на подлежащих контролю объектах, при этом все нарушения категории ε могут иметь место на любом из объектов контроля. Этот случай соответствует «задаче о дробинках, бросаемых случайным образом в N ящиков».

Вероятность того, что количество объектов, на каждом из которых имеется ровно m_ε нарушений ($m_\varepsilon = 0, M_\varepsilon$), составит величину n_{m_ε}, распределена по гипергеометрическому закону:

$$P_{obj}(n_{m_\varepsilon}, n, N) = \frac{C^{n_{m_\varepsilon}}_{[N\cdot p_m]} \cdot C^{n-n_{m_\varepsilon}}_{[N\cdot(1-p_m)]}}{C^n_N}, m_\varepsilon = \overline{0, M_\varepsilon}, \quad (13)$$

где $$p_m = \frac{(\frac{M_\varepsilon \cdot \overline{P}^{(\varepsilon)}_{gen}}{N})^{m_\varepsilon} \cdot e^{-\frac{M_\varepsilon \cdot \overline{P}^{(\varepsilon)}_{gen}}{N}}}{m_\varepsilon !}; \quad (14)$$

[] – знак, определяющий целую часть числа;

$\overline{P}^{(\varepsilon)}_{gen}$ - средняя вероятность возникновения в ИС нарушения требований по ЗИ с категорией ε ,

$$\overline{P}^{(\varepsilon)}_{gen} = \frac{1}{M_\varepsilon \cdot N} \sum_{k=1}^{N} \sum_{i=1}^{M_\varepsilon} P^{(\varepsilon)}_{gen.i}(k) \quad (15)$$

$P^{(\varepsilon)}_{gen.i}(k)$ - вероятность возникновения i -го нарушения требований по ЗИ с категорией ε на k -м объекте в составе ИС.

Среднее количество таких объектов определяется по формуле:

$$\overline{n}_{m_\varepsilon} = \left[n \cdot p_m \right]. \quad (16)$$

Если нарушения выявляются не с единичной вероятностью, то указанные выше формулы модифицируются следующим образом. С учетом того, что количество объектов $n^{(\varepsilon)}_{\text{det}}$, на которых обнаруживаются нарушения с вероятностью $P^{(\varepsilon)}_{\text{det}}$, составляет величину

$$n^{(\varepsilon)}_{\text{det}} = \left[n_{m_\varepsilon} \cdot P^{(\varepsilon)}_{\text{det}} \right], \quad (17)$$

искомая вероятность находится из соотношения:

$$P_{obj}(n_{m_\varepsilon}, n, N, P^{(\varepsilon)}_{\text{det}}) = \frac{C^{n^{(\varepsilon)}_{\text{det}}}_{N\cdot p_m} \cdot C^{n-n^{(\varepsilon)}_{\text{det}}}_{N(1-p_m)}}{C^n_N}, \quad (18)$$

при этом среднее количество объектов, на которых будут обнаруживаться нарушения с категорией ε , определяется по формуле:

$$\overline{n}_{\text{det}}^{(\varepsilon)} = \left[n \cdot p_m \cdot P_{\text{det}}^{(\varepsilon)} \right]. \qquad (19)$$

Расчет второго из указанных показателей среднего уровня (см. рис.1) – вероятности $P_{obj}(n_{\geq m_\varepsilon}, n, N)$ того, что количество объектов, на каждом из которых имеется не менее m_ε нарушений категории ε, составит величину $n_{>m_\varepsilon}$, используется та же модель, однако в формуле (13) вместо вероятности p_m необходимо подставить вероятность $p_{>m}$, рассчитываемую из соотношения:

$$p_{\geq m} = \sum_{j=m_\varepsilon}^{M_\varepsilon} \frac{\left(\frac{M_\varepsilon \cdot \overline{P}_{gen}^{(\varepsilon)}}{N}\right)^j \cdot e^{-\frac{M_\varepsilon \cdot \overline{P}_{gen}^{(\varepsilon)}}{N}}}{j!}. \qquad (20)$$

Из формулы (20) следует, что для объектов, на которых имеется хотя бы одно нарушение, указанная вероятность рассчитывается по формуле:

$$p_{\geq 1} = \sum_{j=1}^{M_\varepsilon} \frac{\left(\frac{M_\varepsilon \cdot \overline{P}_{gen}^{(\varepsilon)}}{N}\right)^j \cdot e^{-\frac{M_\varepsilon \cdot \overline{P}_{gen}^{(\varepsilon)}}{N}}}{j!} \approx 1 - e^{-\frac{M_\varepsilon \cdot \overline{P}_{gen}^{(\varepsilon)}}{N}}. \qquad (21)$$

График зависимости, полученной по формуле (13) для вероятности $P_{obj}(n_{\geq m_\varepsilon}, n, N)$ и некоторых значений параметро в N, M_e и n, приведен на рис.2, из которого видно, что огибающая дискретного распределения вероятности $P_{obj}(n_{\geq m_\varepsilon}, n, N)$ может быть аппроксимировано непрерывным нормальным распределением с параметрами :

$$\overline{n_{i\,1_e}} = n \cdot p_{i\,1} \quad \text{и} \quad D_{i\,1_e} = \frac{N-n}{N-1} \cdot n \cdot p_{i\,1} \cdot (1-p_{i\,1}) \qquad (22)$$

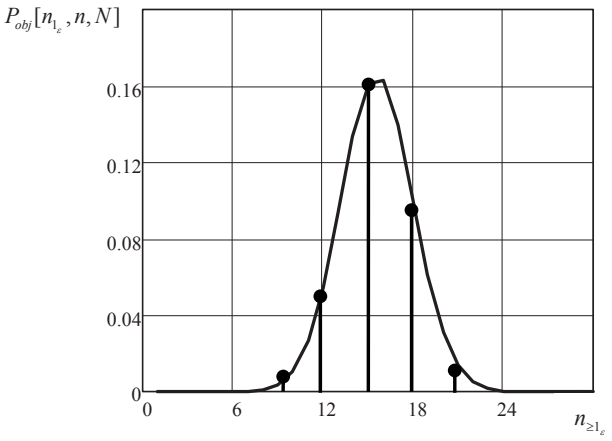

***Рис.2**. График зависимости вероятности того, что количество объектов, на каждом из которых выявляется хотя бы одно нару шение с заданной категорией от количества объектов с нарушениями*

При этом вместо формулы (13) можно использовать формулу:

$$P_{obj}(n_{\geq 1_\varepsilon}, n, N) = \frac{1}{\sqrt{2\pi D_{\geq 1_\varepsilon}}} \cdot e^{-\frac{(\overline{n_{\geq 1_\varepsilon}} - n \cdot p_{\geq 1})^2}{2D_{\geq 1_\varepsilon}}} \qquad (23)$$

На основе изложенной модели может быть рассчитан также и третий из указанных показателей среднего уровня (см. рис.1) – вероятность $P_{obj}(n_{\geq \varepsilon_0}, n, N)$ того, что нарушения с любой категорией, не ниже заданной ε_0, $(\varepsilon \geq \varepsilon_0)$, будут выявлены на $n_{\geq e_0}$ из n проконтролированных объектов в составе ИС. Суть расчета этого показателя сводится к тому, что вместо параметра n_{m_e} используется $n_{\geq e_0}$, а вместо величины M_ε в формуле (20) – величина $M_{\geq \varepsilon_0}$.

С учетом приведенных соотношений может быть рассчитана вероятность того, что в ИС может быть выявлено не более n_e объектов, на каждом из которых имеется хотя бы одно нарушение с категорией ε:

$$P_{obj}(n_\varepsilon, n, N) = \sum_{i=1}^{n_\varepsilon} \frac{C_{[N \cdot p_{\geq 1}]}^{i} \cdot C_{[N \cdot (1-p_{\geq 1})]}^{n-i}}{C_N^n}. \qquad (24)$$

Пример графического представления зависимости (24) для некоторых значений параметров N, M_e и размеров выборки n приведен на рис.3.

Несколько сложнее рассчитывается *четвертый показатель* - вероятность того, что в ИС в ходе контрольных мероприятий будет выявлено не менее заданного количества нарушений заданной совокупности категорий.

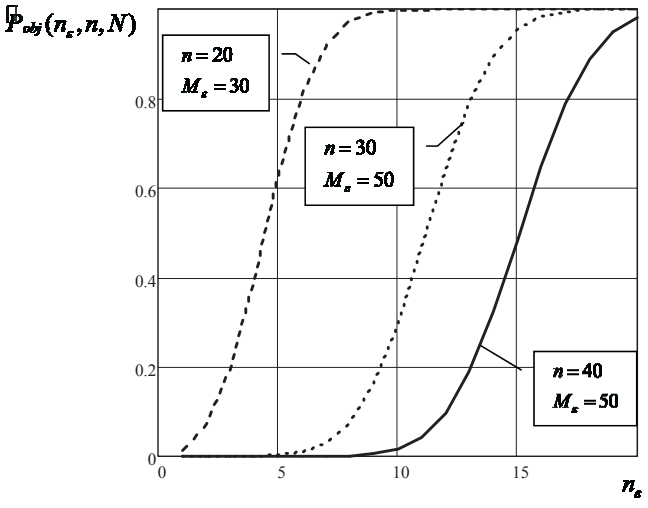

***Рис.3**. Зависимость вероятности того, что в ИС может быть выявлено не более n_ε объектов, на каждом из которых имеется хотя бы одно нарушение с категорией ε, от количества объектов*

Такая вероятность может быть рассчитана при допущении о независимости и равновероятности возникающих нарушений требований по ЗИ с использованием модели «классической задачи о дробинках».

Пусть в составе ИС из N объектов контролируются только $n \le N$ объектов, где n - размер выборки (общее количество выбранных для контроля объектов), при этом в выборку попадают объекты с нарушениями любой категории (или с категорией, не ниже заданной ε_0).

Вероятность того, что в выборке n будут выявлены $m_{\ge e_0}$ нарушений, а оставшиеся $M_{\ge e_0} - m_{\ge e_0}$ нарушений будут иметь место на непроконтролированных $N - n$ объектах, определяется из соотношения (3), [3]:

$$P_{des}(n, m_{\ge e_0}) = C_{M_{\ge e_0}}^{m_{\ge e}} \cdot \frac{n^{m_{\ge e_0}} \cdot (N-n)^{M_{\ge e_0} - m_{\ge e_0}}}{N^{M_{\ge e_0}}}, \quad (25)$$

где $M_{\ge \varepsilon_0}$ - количество возможных нарушений требований по ЗИ с категорией, не менее ε_0,

$$M_{\ge \varepsilon_0} = \sum_{k=1}^{n} \sum_{\varepsilon=\varepsilon_0}^{\varepsilon_{\max}} \sum_{i=1}^{M_\varepsilon(k)} P_{gen.i}^{(\varepsilon)}(k), \quad (26)$$

а вероятность выявления в составе ИС не менее $m_{\ge e_0}^{lim}$ нарушений определяется по формуле:

$$P_{des}(n, m_{\ge e_0}^{\lim}) = \sum_{m_{\ge e}=m_{\ge e_0}^{\lim}}^{M_{\ge e_0}} C_{M_{\ge e}}^{m_{\ge e}} \cdot \frac{n^{m_{\ge e}} \cdot (N-n)^{M_{\ge e_0} - m_{\ge e}}}{N^{M_{\ge e_0}}}. \quad (27)$$

График приведенной зависимости показан на рис.4.

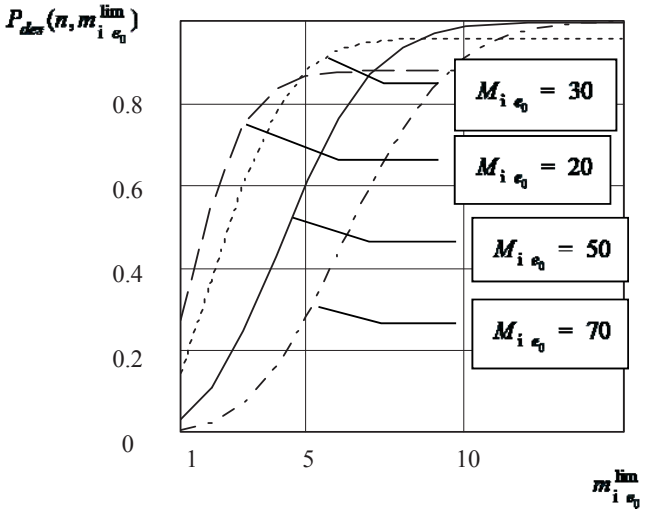

Рис. 4. *Зависимость вероятности выявления не более $m_{\ge e_0}^{\lim}$ нарушений безопасности информации от значения $m_{\ge e_0}^{\lim}$ при различных количествах возможных нарушений $M_{\ge e_0}$*

При этом вероятность выявления в составе ИС не более $m_{\ge e_0}^{\lim}$ нарушений определяется по формуле:

$$\overline{P}_{des}(n, m_{\ge e_0}^{\lim}) = 1 - P_{des}(n, m_{\ge e_0}^{\lim}). \quad (28)$$

Для определения требуемого объема выборки рассмотрим случай, когда для оценки эффективности контроля учитываются все нарушения с категорией ε. В этом случае сначала необходимо рассчитать вероятность того, что получаемая в ходе проведения контрольных мероприятий выборочная величина n_ε отклонится от своего среднего значения на величину δ, которая находится из соотношения (5):

$$P_\Delta\left(\left|\hat{n}_\varepsilon - \overline{n_\varepsilon}\right| < \delta\right) = \Phi\left(\frac{\delta}{\sqrt{2 \cdot \frac{D_{n_\varepsilon}}{n}}}\right), \quad (29)$$

где $\Phi(x)$ - интеграл вероятности (4).

Задавая значение вероятности, можно определить значение δ и доверительный интервал значений Δn_ε:

$$\delta = \sqrt{2 \cdot \frac{D_{n_\varepsilon}}{n}} \cdot \Phi^{-1}(P_\Delta); \quad (30)$$

$$\Delta n_\varepsilon = (\overline{n_\varepsilon} - \delta; \overline{n_\varepsilon} + \delta), \quad (31)$$

где $\Phi^{-1}(P_\Delta)$ - функция, обратная интегралу вероятности Φ.

При этом объем выборки n выбирается такой, чтобы не пропустить с указанной вероятностью нарушения безопасности информации категории ε. Величина n с учетом соотношения (30) и (19) рассчитывается следующим образом:

$$n = \left[\frac{N}{P_{\text{det}}^{(\varepsilon)}} - \frac{\delta^2 \cdot (N-1)}{2 \cdot P_{\text{det}}^{(\varepsilon)} \cdot [\Phi^{-1}(P_\Delta)]^2 \cdot p_{\ge 1} \cdot (1 - p_{\ge 1})}\right], \quad (32)$$

где вероятность $p_{\ge 1}$ определяется из соотношения (20).

Предложенные соотношения позволяют количественно обосновывать объем контрольных мероприятий, если применяется метод однократной выборки.

Литература

1. Платонов Б.Ф., Язов Ю.К., Аксютин В.М. К оценке размеров выборки при контроле безопасности информации в компьютерных системах. / Информация и безопасность. - 2008. Т. 11. № 4. С. 597-600.
2. ГОСТ Р 50922 – 2006. Защита информации. Основные термины и определения.
3. Н.В. Смирнов, И.В. Дунин-Барковский. Курс теории вероятностей и математической статистики для технических приложений. Издание третье. Изд-во «Наука». Главная редакция физико-математической литературы. – М.: 1969.- 512 с.

References

1. Platonov B.F., Iazov Iu.K., Aksiutin V.M. K otsenke razmerov vyborki pri kontrole bezopasnosti informatsii v komp'iuternykh sistemakh. / Informatsiia i bezopasnost'. - 2008. T. 11. № 4. S. 597-600.
2. GOST R 50922 – 2006. Zashchita informatsii. Osnovnye terminy i opredeleniia.
3. N.V. Smirnov, I.V. Dunin-Barkovskii. Kurs teorii veroiatnostei i matematicheskoi statistiki dlia tekhnicheskikh prilozhenii. Izdanie tret'e. Izd-vo «Nauka». Glavnaia redaktsiia fiziko-matematicheskoi literatury. – M.: 1969. 512 s.