СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности (Степаненко Д. А.) («Российский следователь», 2015, N 15)
2. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 9.
3. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификации и квалификации киберпреступлений // Право и кибербезопасность. 2012. N 1. С. 12.
4. Конвенция о преступности в сфере компьютерной информации (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23 ноября 2001 г.) // СПС «КонсультантПлюс» (дата обращения: 12.03.2015).
5. Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014)»Об информации, информатизации и защите информации»
6. Кодекс Республики Беларусь от 09.07.1999 N 275-З (ред. от 20.04.2016)»Уголовный кодекс Республики Беларусь»

СТАТИСТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ РАСПРЕДЕЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. И. ТРУБЕЙ

Учреждение БГУ НИИ прикладных проблем математики и информатики

Для оценки рисков ИБ по формуле $ALE = AV \cdot EF \cdot ARO$ необходимо определить ожидаемую среднегодовую частоту реализации угроз — ARO (AV — стоимость активов, EF — степень уязвимости актива к угрозе). Прогнозируемые частоты реализации угроз (инцидентов ИБ) определяются с применением теории вероятностей и математической статистики, аналитических методов, а также экспертных оценок. Для прогнозирования частот реализации угроз на текущий или будущий годы необходимо проводить анализ угроз на основе накопленных данных об инцидентах ИБ за предыдущие годы. Анализ уязвимостей и угроз, характерных для государственных ИС, может проводиться с использованием банка данных угроз безопасности информации ФСТЭК России. Предлагается метод оценки инцидентов, связанных с реализацией возможных угроз, воздействующих на ИС, с использованием критерия χ^2.

Предположим, что частоты реализации угроз (каналов утечки) $E_1,\ldots,E_i,\ldots,E_N$ за отрезки времени $t_1,\ldots,t_k,\ldots,t_M$ (например, за квартал, год) составляют $\nu_{k,1},\ldots,\nu_{k,i},\ldots,\nu_{k,N}$ ($\nu_{k,i}$ — частота реализации угрозы E_i за отрезок времени t_k). Получим M независимых выборок, каждая из которых есть реализация некоторой полиномиальной схемы с исходами $1,\ldots,N$. Объемы выборок равны $z_1,\ldots,z_M$; $z = \sum_{k=1}^{M} z_k$, $t_0 = min\{z_1,\ldots,z_M\}$.

Выясним, происходили ли изменения в распределении вероятностей реализации угроз во временных промежутках $t_1,\ldots,t_k,\ldots,t_M$, т.е. проверим однородность выборок. Для проверки однородности полиномиальных выборок обычно используют статистику χ^2.

$$\chi^2 = \sum_{k=1}^{M}\sum_{i=1}^{N}\frac{\left(\nu_{k,i} - z_k m_i / z\right)^2}{z_k m_i / z} = z\sum_{k=1}^{M}\sum_{i=1}^{N}\frac{1}{z_k m_i}\left(\nu_{k,i} - m_i\frac{z_k}{z}\right)^2, \quad (1)$$

где $m_i = \sum_{k=1}^{M}\nu_{k,i}$.

При $z_0 \to \infty$ данная статистика сходится по распределению к случайной величине $\chi_{(M-1)(N-1)}$, имеющей распределение хи-квадрат с $(M-1)(N-1)$ степенями свободы. Проверяемая гипотеза принимается, когда значение статистики χ^2 не превышает критического значения χ_p^2, или достигнутый уровень значимости больше заданного уровня значимости p. Для всех ожидаемых частот должно соблюдаться условие: $t_k p_{k,i} \geq 5$.

Представляют интерес частные случаи формулы (1). При $M = 2$ мы будем иметь 2 независимые выборки, $N-1$ степеней свободы и формула примет вид:

$$\chi_{k,l}^2 = z_k z_l \sum_{i=1}^{N}\frac{1}{\nu_{k,i} + \nu_{l,i}}\left(\frac{\nu_{k,i}}{z_k} - \frac{\nu_{l,i}}{z_l}\right)^2, \quad (2)$$

где $\nu_{k,1},\ldots,\nu_{k,N}$; $\nu_{l,1},\ldots,\nu_{l,N}$ — наборы частот соответственно k-й и l-й выборок; $z_k = \sum_{i=1}^{N}\nu_{k,i}$; $z_l = \sum_{i=1}^{N}\nu_{l,i}$.

При $N = 2$ мы будем иметь M последовательных наблюдений, в каждом из которых угроза l осуществляется соответственно $\nu_1,\nu_2,\ldots,\nu_j,\ldots,\nu_M$ раз. Проверяется гипотеза о том, что угроза l во всех наблюдениях имеет одну и ту же, постоянную вероятность p. и Формула для статистики хи-квадрат (с $M-1$ степенями свободы) примет вид:

$$\chi^2 = \sum_{j=1}^{M}\frac{\left(\nu_j - z_j p^*\right)^2}{z_j p^* q^*} = \frac{1}{p^* q^*}\sum_{j=1}^{M}\frac{\nu_j^2}{z_j} - z\frac{p^*}{q^*}, \quad (3)$$

где $p^* = 1 - q^* = \frac{1}{t}\sum_{j=1}^{M}\nu_j$.

Если выборки «близки» к однородным, то статистика χ^2 будет иметь нецентральное распределение хи-квадрат с тем же числом степеней свободы и ее значение будет пропорционально объему выборки. Использование больших выборок может привести к решению об отклонении гипотезы H_0, хотя неоднородность выборок может быть несущественной и иногда ею можно пренебречь. В статистических приложениях широко используют различные приближения с помощью «центрального» хи-квадрат распределения и нормального распределения.

Проиллюстрируем применение предложенного метода на примере отчетов JSOC Security flash report, которые основаны на данных, полученных в коммерческом центре мониторинга и реагирования на инциденты информационной безопасности — Solar JSOC. По информации руководства компании в настоящее время к Solar JSOC подключено более 20 клиентов: предприятия энергетики, финансовые организации, транспортные компании. При формировании выборок будем рассматривать не суммарные частоты инцидентов, зафиксированные компанией Solar JSOC, а средние частоты реализации угроз на каждого клиента компании. Для определенности количество клиентов будем считать равным 20.

1. Распределение инцидентов по внешним и внутренним

Проверим, совместимы ли приведенные в таблице 1 данные с гипотезой о том, что, реализация внутренних, а, следовательно, и внешних угроз в указанные промежутки времени имеют одни и те же вероятности.

Таблица 1

Частоты внешних и внутренних инцидентов

Инциденты	3 кв. 2014	4 кв. 2014	1 кв. 2015	2 кв. 2015	3 кв. 2015	4 кв. 2015	χ^2_5
Внешние	358	480	623	866	950	869	10,5
Внутренние	585	984	1115	1528	1779	1703	10,5
Всего	943	1464	1738	2394	2729	2572	

Вычислим значение статистики χ^2 по формуле (3) для $N = 2$. Получим χ^2, что лежит ниже уровня значимости $p = 0,05$ с четырьмя степенями свободы, равного 11,1, и можно считать, что указанная гипотеза справедлива.

2. Внешние инциденты

Инициаторами и причиной внешних инцидентов являются действия лиц, не являющихся внутренними пользователями. Частоты инцидентов приведены в таблице 2.

Таблица 2

Направления атак внешних инцидентов

Суммарные частоты внешних инцидентов		Частоты внешних инцидентов по направлениям атак					
		E_1	E_2	E_3	E_4	E_5	E_6
		Атаки на web-прилож.	Brute-force и компр. уч. данных внеш. серв.	Компр. админ. учетных записей	Атаки на управл. протоколы систем	DDoS-атаки	Прочие внешние атаки
4 кв. 2015	869	358	156	25	45	39	246
3 кв. 2015	950	371	209	20	60	31	259
2 кв. 2015	866	380	217	28	60	19	162
1 кв. 2015	623	263	169	16	45	10	120
4 кв. 2014	480	188	106	10	30	16	130
3 кв. 2014	358	136	92	5	19	10	96
χ^2_{25} = 90,4		χ^2_5 =6,9	χ^2_5 =22,9	χ^2_5 =5,1	χ^2_5 =3,9	χ^2_5 =13,1	χ^2_5 =38,5

Оценим однородность полученных выборок. В таблице 2 приведены значения статистик χ^2, вычисленных по формуле (1) (для суммарных выборок при M =6, N =6) и по формуле (3) (для частот конкретных инцидентов при M =6, N =2). Значения статистик свидетельствуют о том, что происходили определенные (однако не существенные) изменения в распределении вероятностей реализации внешних угроз в указанные промежутки времени. При этом вероятности реализации угроз E_1, E_3, E_4, практически не изменялись. При сравнении выборок инцидентов за последний (четвертый) квартал 2015 года с третьим кварталом по формуле (2) получим χ^2_5=8,3 (для пяти степеней свободы), которое означает, что в течение данных кварталов не произошло существенных изменений в распределении внешних инцидентов.

3. Внутренние инциденты

Инициаторами и причиной внутренних инцидентов являются действия внутренних сотрудников: халатность в соблюдении политик ИБ или их прямое нарушение, компрометация или передача учетных данных сотрудников, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем. К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра. Частоты данных инцидентов по направлениям атак приведены в таблице 3.

Таблица 3

Направления атак внутренних инцидентов

Суммарные частоты внутренних инцидентов		**Частоты внутренних инцидентов по направлениям атак**					
		E_1	E_2	E_3	E_4	E_5	E_6
		Утечки конф. данных	**Вирусные атаки**	**Компр. учетных записей**	**Нарушение политик доступа в Интернет**	**Нелегит. работы под привилегир. учетными записями**	**Нелегит. изменения в IT-системах, несанкц. активн, удал. доступа, прочее**
4 кв. 2015	1703	685	245	225	198	105	245
3 кв. 2015	1779	630	231	209	278	132	299
2 кв. 2015	1528	433	294	236	170	93	302
1 кв. 2015	1115	337	190	180	138	60	210
4 кв. 2014	984	349	128	115	154	73	165
3 кв. 2014	585	151	69	82	72	64	117
χ^2_{25} = 206,2		χ^2_5 =78,2	χ^2_5 =39,0	χ^2_5 =19,1	χ^2_5 =24,9	χ^2_5 =23,2	χ^2_5 =21,8

Значения статистик χ^2, приведенных в таблице 3 свидетельствуют о том, что происходили существенные изменения в распределении вероятностей внутренних угроз в указанные промежутки времени.

В таблице 4 приведено распределение частот внутренних инцидентов по каналам утечек, а также соответствующие значения статистик χ^2 для суммарных выборок и для конкретных каналов утечек.

Таблица 4

Распределение внутренних инцидентов по каналам утечек

Суммарные частоты внутренних инцидентов		**Частоты внутренних инцидентов по каналам утечек**				
		E_1	E_2	E_3	E_4	E_5
		Устройства доступа в Интернет	**Электронная почта**	**Веб-ресурсы**	**Съемные носители**	**Печать**
4 кв. 2015	1703	291	550	364	334	164
3 кв. 2015	1779	279	555	420	307	218
2 кв. 2015	1528	219	449	417	284	159
1 кв. 2015	1115	144	294	353	225	99
χ^2_{20} = 81,9		χ^2_4 =10,4	χ^2_4 =12,6	χ^2_4 =45,5	χ^2_4 =4,9	χ^2_4 =10,4

Значения статистик χ^2 свидетельствуют о том, что происходили определенные (однако не существенные) изменения в распределении вероятностей каналов утечек в указанные промежутки времени.

Метод может использоваться для выявления тенденций в динамике угроз. Если при сравнении частот инцидентов ИБ за текущий квартал, полугодие, год с частотами инцидентов за прошлый квартал, полугодие, год не выявлено существенного изменения в распределении вероятностей инцидентов (значение статистики χ^2 не превышает заданного уровня), то с определенной вероятностью можно предположить, что эти показатели будут стабильны в среднесрочной перспективе. Это позволит спрогнозировать потенциальные частоты инцидентов на будущий год, которые, в свою очередь, могут быть использованы при оценке рисков ИБ. Если же значение статистики χ^2 однородности значительно превышает заданный уровень, то необходимо выявлять причины сложившейся ситуации с изменением распределения инцидентов и проводить углубленный анализ угроз, воздействующих на ИС.