УДК 519.2

ЭНТРОПИЙНЫЙ АНАЛИЗ СТОЙКОСТИ ИТЕРАЦИОННОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ФЕЙСТЕЛЯ

О.С.КИВЕЛЬ, Ю.С.ХАРИН

НИИ прикладных проблем математики и информатики, Белорусский государственный университет, г. Минск, 220030, Республика Беларусь

0. Введение

Согласно теории Шеннона [1] совершенные криптосистемы должны использовать в качестве ключевой последовательности равномерно распределенную случайную последовательность (РРСП), которую на практике называют «чисто случайной последовательностью». РРСП определяется двумя вероятностными свойствами: случайные величины произвольного набора независимы в совокупности; любая случайная величина имеет дискретное равномерное распределение вероятностей [2, 3]. Генерация «чисто случайной» последовательности подразумевает высокую сложность и значительные материальные затраты. В сложившейся в мире ситуации массового применения шифрования, связанной с использованием сети Интернет и передачи информации с ее помощью, не всегда выполняется условие равномерного распределения случайной последовательности [3]. Это удешевляет безопасность, но служит причиной ухудшения стойкости используемых криптосистем. Данная статья развивает результаты статьи [4], в которой исследовались вероятностные характеристики итерационного криптографического преобразования Фейстеля в зависимости от вероятностного распределения ключа. Здесь исследуем проблему стойкости со стороны энтропийных характеристик.

1. Математическая модель.

Интерес для исследования представляет вопрос зависимости результирующего шифртекста от фиксированного входного сообщения с учетом ключевого расписания и его энтропийных характеристик. Примем обозначения для математического описания итерационного криптографического преобразования Фейстеля:

$V \in \{0,1\}$ – двоичный алфавит;

$X = (X_1,...,X_N) \in V^N$ – произвольный фиксированный текст, представляющий собой последовательность символов из алфавита V;

$Y^{(t)} = (Y_1^{(t)},...,Y_N^{(t)}) \in V^N$ – результат преобразования исходного текста X после t тактов;

$K \in V^M$, $K = (K_1 \| K_2 \| ... \| K_L)$, $K_i \in V^m$, $i = 1,2,...,L$, $M = L \cdot m$, – ключ, разбитый на L подключей $K_1,...,K_L \in V^m$ длины m;

$\{k_1,...,k_L,k_{L+1},...,k_{L+\tau}\}$ – ключевое расписание для $L + \tau$ тактов алгоритма шифрования, причем подключи имеют длину m и начиная с $L + 1$-го подключа «повторяются»:

$k_t \in \{K_1,...,K_L\}$, $t = L+1,...,L+\tau$,

или в более общей ситуации функционально выражаются через $K_1,...,K_L$:

$$k_t = \mathcal{X}_t(K_1,\ldots,K_L),\ t = L+1,...,L+\tau, \qquad (1)$$

где $\mathcal{X}_t(\cdot): V^{m+L} \to V^m$ – заданная детерминированная функция;

$Y^{(t)} = (Y_1^{(t)},...,Y_N^{(t)}) = F_x(k_1,...,k_t) = G(Y^{(t-1)};k_t) \in V^N$, $t = 1,2,...,L+\tau$, (2)

– преобразование исходного текста $X \in V^N$ после t тактов, где $Y^{(0)} ::= X$, $F_x(k_1,...,k_t)$ – преобразование Фейстеля на t-ом такте, а $G(\cdot)$ – тактовая функция;

$Y^{(L+\tau)} = F_x(k_1,...,k_{L+\tau})$ – выходной шифртекст.

2.Исследование динамики энтропии случайного вектора $Y^{(t)}$.

Для анализа стойкости криптографического преобразования $F_x(\cdot)$, определяемого (2), будем использовать теоретико-информационный подход Шеннона [1, 2].

Пусть $K_1, K_2,..., K_L$ независимые и одинаково распределенные случайные векторы (подключи) с некоторым распределением вероятностей:

$P\{K_i = J\} = p_J$, $J \in V^m$.

Обозначим энтропию Шеннона для подключа K_1 через $h = H\{K_1\}$:

$$H\{K_1\} = -\sum_{J \in V^m} p_J \cdot \log_2 p_J .$$

Учитывая, что V – двоичный алфавит, имеем оценку энтропии h: $0 \le h \le m$. В силу независимости и одинаковой распределенности K_1, K_2,..., K_L энтропия каждого подключа принимает значение h.

Теорема 1. Если $t \cdot h$ и $L \cdot h$ не превосходит N, а K_1, K_2,..., K_L независимые и одинаково распределенные случайные векторы с энтропией h и ключевым расписанием, удовлетворяющим (1), то

$$H\{k_1,...,k_t\} = \begin{cases} t \cdot h, \text{ если } 0 \le t \le L, \\ L \cdot h, \text{ если } L+1 \le t \le L+\tau. \end{cases}$$

Доказательство. По свойству аддитивности энтропии [5] при $1 \le t \le L$ получаем:

$$H\{k_1,...,k_t\} = H\{k_1\} + ... + H\{k_t\} = \underbrace{h + ... + h}_{t} = t \cdot h .$$

Так как согласно (1) подключи начиная с $L + 1$ функционально выражаются через K_1,..., K_L, то учитывая, что при дискретном функциональном преобразовании энтропия не возрастает [5], для $L + 1 \le t \le L + \tau$ имеем:

$$H\{k_1,...,k_t\} = H\{k_1\} + ... + H\{k_L\} + H\{k_{L+1}\} + ... + H\{k_{L+\tau}\} = \underbrace{h + ... + h}_{L} = L \cdot h .$$

Теорема 2. Если имеет место итерационное преобразование (2) и выполняются условия Теоремы 1, то при фиксированном $X \in V^N$ для энтропии случайного вектора $Y^{(t)}$ справедливо соотношение:

$$H\{Y^{(t)}\} \le \min\left\{N, \begin{cases} t \cdot h, \text{ если } 0 \le t \le L, \\ L \cdot h, \text{ если } L+1 \le t \le L+\tau \end{cases}\right\}.$$

Доказательство. $k_1,...,k_t$ подвергаются дискретному функциональному (ДФП) преобразованию $F_x(k_1,...,k_t)$. В силу теоремы о ДФП энтропии [5] и Теоремы 1 получим:

$$H\{Y^{(t)}\} = H\{F_x(k_1,...,k_t)\} \le H\{k_1,...,k_t\} = \begin{cases} t \cdot h, \text{ если } 0 \le t \le L, \\ L \cdot h, \text{ если } L+1 \le t \le L+\tau. \end{cases}$$

С другой стороны энтропия случайного вектора $Y^{(t)}$ принимает максимальное значение при равномерном распределении вероятностей $k_1,...,k_t$ (энтропия Хартли):

$$H\{Y^{(t)}\} = H\{F_x(k_1,...,k_t)\} \le N .$$

Следствие. Если в условиях Теоремы 2 существует $1 \le l^* \le L$ такое, что

$$m \cdot l^* = N \tag{3}$$

и функция $Y^{(l^*)} = F_x(k_1,...,k_{l^*})$ является биекция $Y^{(l^*)} \leftrightarrow (k_1,...,k_{l^*})$, то

$$H\{Y^{(t)}\} = \begin{cases} t \cdot h, \text{если } 1 \le t \le l^*, \\ \le N, \text{если } l^* \le t \le L + \tau. \end{cases}$$

Доказательство. В силу Теоремы 2 и $L \cdot h < N$ имеем:

$$H\{Y^{(t)}\} = \begin{cases} t \cdot h, \text{если } 0 \le t \le L, \\ \le N, \text{если } L+1 \le t \le L + \tau. \end{cases}$$

Учитывая утверждение (3), равенство $M = L \cdot m$ и биективность функции $Y^{(l^*)} = F_x(k_1,...,k_{l^*})$, получаем:

$$H\{Y^{(t)}\} = \begin{cases} t \cdot h, \text{если } 1 \le t \le l^*, \\ \le N, \text{если } l^* \le t \le L + \tau. \end{cases}$$

Из Теоремы 2 и Следствия заключаем, что линейный рост энтропии $H\{Y^{(t)}\}$ наблюдается начиная с такта $t = 1$ по l^*-ый такт. С такта $t = l^* + 1$ по $t = L$ скорость роста снижается и зависит от конкретного вида G (·), а с $t = L + 1$ по $t = L + \tau$ – энтропия не изменяется. Эта динамика энтропии $H\{Y^{(t)}\}$ иллюстрируется на рисунке 1.

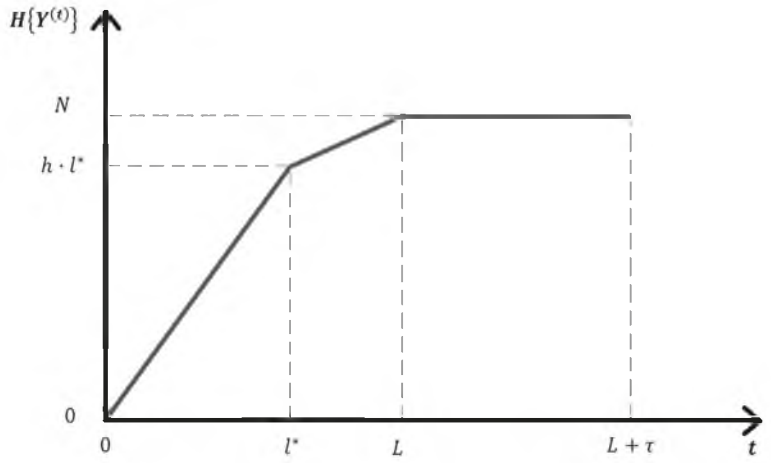

Рисунок 1. Рост энтропии $H\{Y^{(t)}\}$ зависимости от номера такта t

Рассмотрим некоторые частные случаи.

Случай 1. Если $h = m$, т.е. энтропия подключа равна максимальному возможному значению, то в силу (3) на такте номер $t = l^* \le L$ энтропия $H\{Y^{(t)}\}$ достигает максимально возможное значение (см. рис. 2):

$$\max\{H\{Y^{(l^*)}\}\} = N.$$

В этом случае линейный рост энтропии $H\{Y^{(t)}\}$ наблюдается с *1*-го по l^*-ый такт, и далее $t = l^* + 1$ по $t = L + \tau$ энтропия не изменяется и равна N.

Отметим, что в силу (3):

$$l^* = \frac{N}{m}$$

Пример 1.1. Для ГОСТ 28147-89 [2]:
$N = 64$, $L = 8$, $m = 32$, $M = 256$, $\tau = 24$, $l^* = 2$.

Пример 1.2. Для государственного стандарт симметричного шифрования и контроля целостности Республики Беларусь [6]:
$N = 128$, $L = 8$, $m = 32$, $M = 256$, $\tau = 46$, $l^* = 4$.

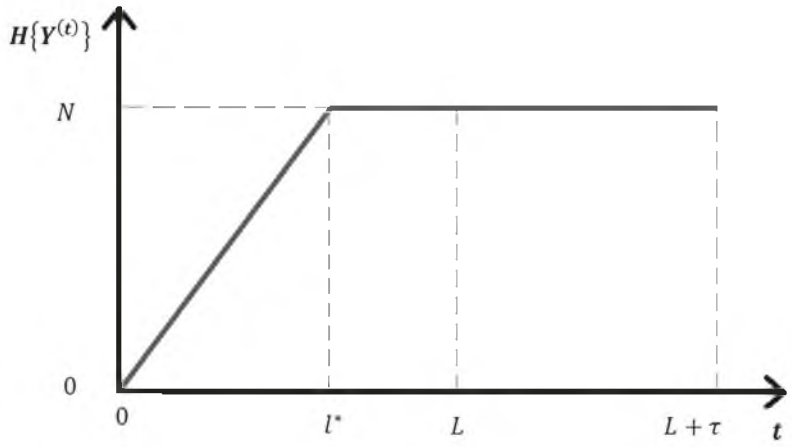

Рисунок 2. Случай $h = m$

Случай 2. Если же выполняется $h \cdot < L < N$, тогда динамика энтропии $Y^{(t)}$ описывается следующим соотношением:

$$H\{Y^{(t)}\} = \begin{cases} t \cdot h, \text{если } t \in \{1,...,L\}, \\ h \cdot L \le N, \text{если } t \in \{L+1,...,L+\tau\}. \end{cases}$$

Пример 2.1. Для ГОСТ 28147-89 рассмотрим такие ключевые последовательности, что $h = 1$. Тогда динамика энтропии $Y^{(t)}$ имеет вид:

$$H\{Y^{(t)}\} = \begin{cases} t, \text{если } t \in \{1,...,8\}, \\ 8, \text{если } t \in \{9,...,32\}. \end{cases}$$

Такая ситуация может возникать следующим образом. Пусть $\xi_1,...,\xi_8 \in V$ – независимые одинаково распределенные случайные величины Бернулли с распределением вероятностей $\mathcal{L}\{\xi_i\} = Bi\left(1,\frac{1}{2}\right)$, $i = 1,...,8$ и $K_i = \left(\xi_i, \overline{\xi_i}, \xi_i, \overline{\xi_i}, ..., \xi_i, \overline{\xi_i}\right)$, где $\overline{\xi_i} = 1 - \xi_i$, то зависимость между $H\{Y^{(t)}\}$ и t будет линейной до $L = 8$ такта, а далее энтропия перестанет изменяться (см. рис. 3).

3. Связь вероятности ошибки прогнозирования с энтропией

Энтропийные свойства криптографического преобразования Фейстеля, рассмотренные в предыдущих разделах, связаны со стойкостью криптосистемы к криптоанализу. Если криптопреобразование таково, что при заданном распределении вероятностей случайного ключа $P(K)$ распределение вероятностей $P\{Y \mid X\} \equiv 2^{-N}$ является равномерным, то оно

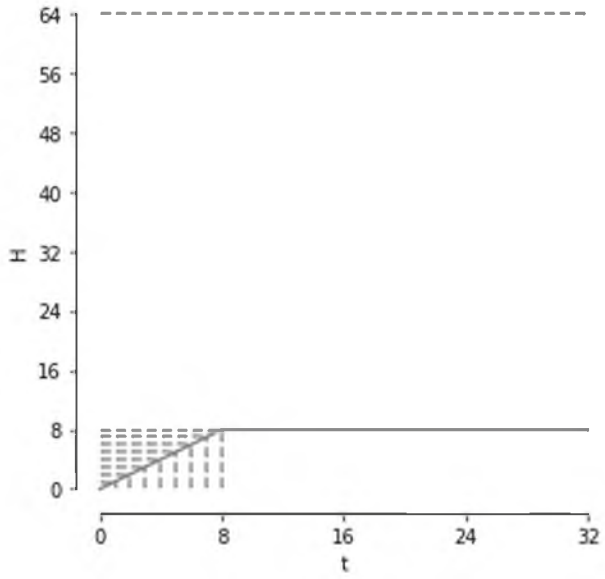

Рисунок 3. $h = 1$

является криптостойким, и, наоборот, если $P\{Y \mid X\} \in \{0,1\}$ равно или *0*, или *1*, то Y и X связаны детерминированно, то преобразование имеет нулевую криптостойкость. Поэтому исследуем вероятность ошибки предсказания Y по X при случайном ключе в зависимости от энтропии ключа $H\{K\}$.

Рассмотрим простейший случай, когда Y принимает лишь два значения, т.е. $Y \in V = \{0,1\}$. Тогда при фиксированном X случайная величина $Y \in \{0,1\}$ имеет распределение Бернулли $Bi(1, p)$:

$p = P\{Y = 1\}$, $q = 1 - p = P\{Y = 0\}$,

где p – некоторый параметр, вообще говоря зависящий от X.

Пусть при фиксированном X получена выборка $\{Y_1,..., Y_n\}$ объема n. Построим состоятельную, асимптотически нормальную, несмещенную оценку:

$$\hat{p} = \frac{1}{n}\sum_{i=1}^{n} Y_i \in [0,1].$$

Теорема 3. Если при фиксированном X случайная величина $Y \in \{0,1\}$ имеет распределение Бернулли $Bi(1, p)$, $p = P\{Y = 1\}$, $q = 1 - p = P\{Y = 0\}$, то наименьшая вероятность ошибки прогнозирования равна

$$q_n(p) = \sum_{i=0}^{n/2} C_n^i \cdot p^i \cdot (1-p)^{n-i}$$

и имеет асимптотическое приближение при $n \to \infty$:

$$q_n(p) \approx \Phi\left(-\sqrt{n}\frac{p-\frac{1}{2}}{\sqrt{p(1-p)}}\right) \xrightarrow[n\to\infty]{} 0.$$

Доказательство. Наименьшая вероятность ошибки достигается для следующей статистики [7]:

$$\hat{Y} = \begin{cases} 1, если\ \hat{p} \geq \dfrac{1}{2}, \\ 0, если\ \hat{p} < \dfrac{1}{2}. \end{cases}$$

Вычислим вероятность ошибки прогнозирования при истинном значении $p \geq \frac{1}{2}$:

$$q_n(p) := P\left\{\hat{p} < \frac{1}{2}\right\} = P\left\{n\hat{p} < \frac{n}{2}\right\} = \mathcal{L}\{n\hat{p}\} = Bi(n, p) = \sum_{i=0}^{n/2} C_n^i \cdot p^i \cdot (1-p)^{n-i}.$$

Тогда в силу ЦПТ [7] $Bi(n, p) \approx Bi(np, npq)$ для $n >> 1$:

$$q_n(p) \approx \Phi\left(\frac{\frac{n}{2} - np}{\sqrt{np(1-p)}}\right) = \Phi\left(-\sqrt{n}\frac{p - \frac{1}{2}}{\sqrt{p(1-p)}}\right) \xrightarrow[n\to\infty]{} 0.$$

На рисунке 4 представлен график зависимости точной вероятности ошибки прогнозирования $q_n(p)$ для разного объема выборки n от значения вероятности p.

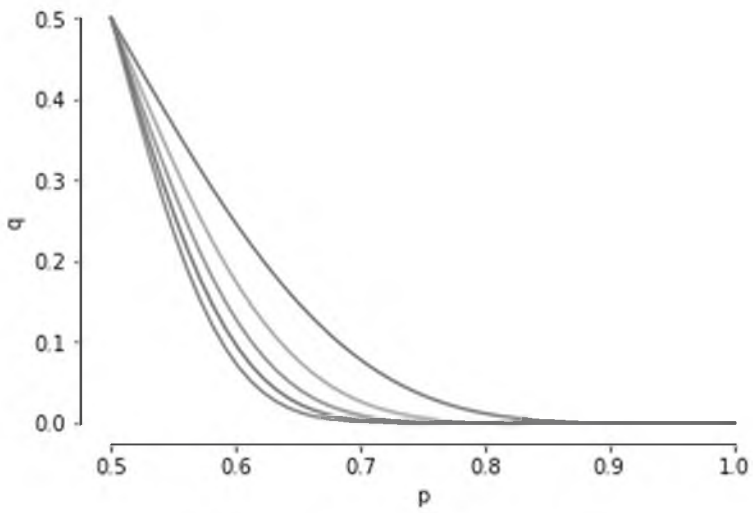

Рисунок 4. Зависимость $q_n(p)$ от вероятности p n = 11, 21,...,51

Определим обратную функцию $\psi(\cdot): \{0,1\} \to \{0,1\}$ такую, что:
$p = \psi(h)$, $H_{\psi(h)} \equiv h$.

Зависимость между энтропией H_p и вероятность «успеха» p представлена на рисунке 5.

Следствие. Вероятность ошибки прогнозирования $q_n(p)$ можно представить в следующем асимптотическом виде при $n \to \infty$:

$$q_n(p) \approx \Phi\left(-\sqrt{n}\frac{\psi(h) - \frac{1}{2}}{\sqrt{\psi(h)(1-\psi(h))}}\right) := Q_n(h).$$

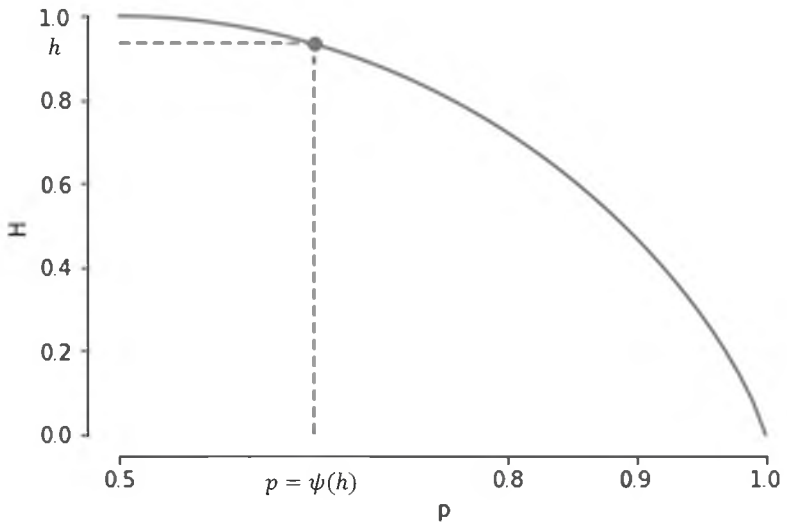

Рисунок 5. Зависимость H_p от вероятности p

Построенная функция $Q_n(h)$ определяет монотонную зависимость вероятности ошибки прогнозирования от энтропии h. График этой функции для различного объема выборки n представлен на рисунке 6.

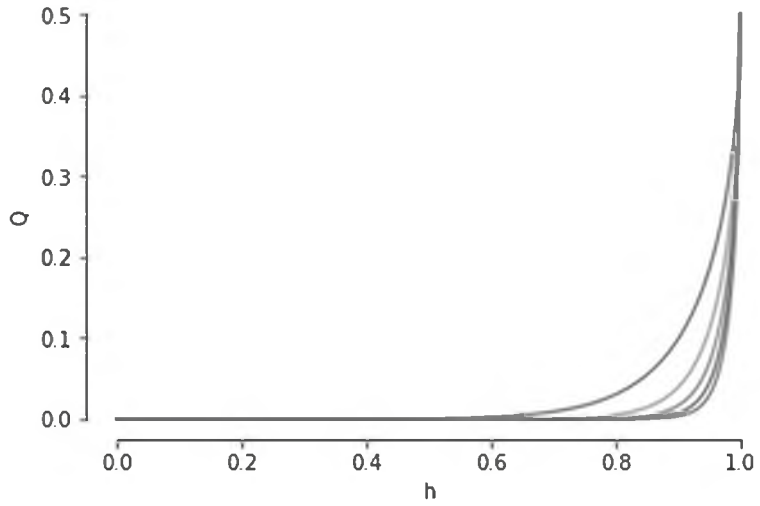

Рисунок 6. Зависимость $Q_n(h)$ от энтропии h n = 11, 21,...,51

Список литературы

1. Shannon, C. E. A Mathematical Theory of Communication / C.E. Shannon // Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948
2. Криптология: учебник / Ю.С.Харин, С.В.Агиевич, Д.В.Васильев, Г.В.Матвеев – Минск: БГУ, 2013.

3. L'Ecuyer, P. History of uniform random number generation. In Proceedings of the WSC 2017 – Winter Simulation Conference, Las Vegas, NV, USA, 3-6 Deccember 2017.
4. Кивель, О. С. Вероятностный анализ стойкости итерационного криптографического преобразования Фейстеля / О.С.Кивель, Ю.С.Харин // Комплексная защита информации: материалы XXIV науч.-практ. конф., Витебск, 21-23 мая 2019 г. – Витебск : ВГТУ, 2019 – С. 232 – 238
5. Математические основы теории информации : учеб. пособие / Ю. С. Харин, И. А. Бодягин, Е. В. Вечерко. – Минск : БГУ, 2018. – 19 с.
6. Криптографические алгоритмы шифрования и контроля целостности: СТБ 34.101.31–2007. – Введ. 31.01.2011. – Минск: Госстандарт, 2011– 4 с.
7. Теория вероятностей, математическая и прикладная статистика : учебник / Ю. С. Харин, Н. М. Зуев, Е. Е. Жук. – Минск: БГУ, 2011.

УДК 004.056

ПОДХОД К РЕАЛИЗАЦИИ СИСТЕМЫ ЭМУЛЯЦИИ ДЕЙСТВИЙ НАРУШИТЕЛЯ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИБ

Д.М. КОРОЛЬ

«МИРЭА – Российский технологический университет»
г. Москва, 119454, Российская Федерация

Введение

Вопросы, связанные с прикладным решением задач в сфере информационной безопасности, набирают свою актуальность. С развитием информационных технологий многие теоретические, ранее недоступные для реализации, средства воплощаются в жизнь. Однако они порождают множество уязвимостей, связанных с ними. В этой связи компетентный специалист по информационной безопасности должен уметь находить уязвимости, и подтверждать возможность их эксплуатации. В докладе представлены концепция, проведения практических занятий и описаны средства её реализации, оптимизирующие процесс освоения студентами практических навыков за счёт автоматизации затратных по времени этапов, таких как разведка сети и формирование полезной нагрузки. Предлагаемое архитектурное решение обеспечивает непереносимость средств эксплуатации уязвимостей без основательной переработки. В работе кратко описаны архитектура и функционал экспериментального киберполигона «Купол», частью которого является разработанная система эмуляции действий нарушителя. Автором рассмотрены требования для разработанной системы, описаны её основные модули и рассмотрены особенности их реализации. Дополнительны приведены возможные сценарии проведения практических занятий на киберполигоне «Купол» и роль спроектированной системы в них.