DOI 10.37882/2223-2966.2025.04-2.19

ПОДХОД К ОБЕСПЕЧЕНИЮ НАДЕЖНОСТИ РАБОТЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

APPROACH TO ENSURING RELIABILITY OF CORPORATE INFORMATION SYSTEMS

L. Maleshina
A. Dubrovsky

Summary. In the conditions of the modern digital economy, corporate information systems, ensuring reliability and competitiveness, have become an integral part of the successful functioning of organizations and enterprises. The introduction of innovative technologies and equipment has allowed not only to improve the management of information, resources and business processes in various fields of activity, but also expanded the landscape of information security threats. The article substantiates the need to modernize computer attack detection systems, which may result in critical situations that disrupt the normal operation of systems. The problem of combining the readings of several detection tools and making a decision on the presence or absence of a threat on their basis is presented. A method for solving it is proposed, based on the concept of a «critical area», taking into account the individual characteristics of information threat detection tools.

Keywords: corporate information system, reliability, information security, information threat, threat detection tool.

Малёшина Людмила Михайловна
Кандидат технических наук, доцент,
Российский университет транспорта (МИИТ), Москва
docentmlm@mail.ru
Дубровский Арсений Александрович
Российский университет транспорта (МИИТ), Москва

Аннотация. В условиях современной цифровой экономики корпоративные информационные системы, обеспечивая надежность и конкурентоспособность, стали неотъемлемой частью успешного функционирования организаций и предприятий. Внедрение инновационных технологий и техники позволило не только усовершенствовать управление информацией, ресурсами и бизнес-процессами в различных сферах деятельности, но и расширило ландшафт угроз информационной безопасности. В статье обоснована необходимость модернизации систем обнаружения компьютерных атак, вследствие которых могут возникать критические ситуации, нарушающие нормальную работы систем. Представлена задача объединения показаний нескольких средств обнаружения и принятия на их основе решения о наличии угрозы или отсутствии таковой. Предложен способ ее решения, основанный на понятии «критической области», учитывающий индивидуальные характеристики средств обнаружения информационных угроз.

Ключевые слова: корпоративная информационная система, надежность, информационная безопасность, информационная угроза, средство обнаружения угроз.

Эффективное функционирование и расширение сферы деятельности рынка возможно только при наличии «конкуренции», так как конкуренция выступает важным фактором для экономического развития [1]. В современных условиях «конкурентоспособность» стала одной из основополагающих идей при разработке экономической политики любого субъекта рыночных отношений [2]. Что делает доминирующей потребность организаций и предприятий непрерывно улучшать характеристики выпускаемой продукции или оказываемых услуг, формируя, таким образом, ключевые преимущества над конкурентами.

Среди наиболее действенных способов повышения качества работы предприятия можно выделить следующие:

- поиск новых методов экономического планирования;
- повышение оперативности управления производством;
- реструктуризация управления финансовыми потоками;
- эффективное использование ресурсов предприятия;
- снижение доли издержек.

В условиях постоянно усиливающейся конкуренции рост добавленной стоимости в выпуске продукции возможен только при наличии у предприятия компетентных преимуществ, формируемых путем внедрения в производственные процессы инновационных технологий и техники [2]. Таким образом корпоративные информационные системы (далее — КИС), предоставляющие собой комплексное и эффективное управление информацией, ресурсами и бизнес-процессами, обеспечивая надежность и конкурентоспособность в быстро меняющемся цифровом мире, стали неотъемлемой частью успешного функционирования организаций и предприятий.

Но «цифровая трансформация» не только позволяет усовершенствовать решение задач планирования и управления различными видами деятельности, но и расширяет ландшафт угроз информационной безопасности. По данным компании Positive Technologies «в 2022 году случился всплеск атак на российские организации ввиду ухудшения геополитической ситуации, что повлияло на ландшафт киберугроз всей страны. За первые три квартала 2024 года количество успешных атак практически сравнялось с показателями за весь 2022 год.

Российские организации атакуются десятками кибершпионских, хактивистских и финансово мотивированных группировок» [3]. В 2023 году увеличилось число успешных атак на организации по всему миру [4]. В III квартале 2024 года, как и в предыдущих кварталах, компьютерные преступники сосредоточили свое внимание на краже конфиденциальной информации (рис. 1). Несанкционированное раскрытие очень важных для организации, ее клиентов и контрагентов сведений впоследствии могут привести к финансовым потерям, прерыванию бизнес-процессов или работоспособности отдельных систем, а также к последующим атакам на контрагентов и частных лиц.

Ввиду перманентно высокого уровня атак на КИС, актуальной остается задача минимизации ущерба при нарушении нормальной работы системы, решение которой возможно только при своевременном и как можно более раннем выявлении несанкционированных действий нарушителей.

Для определения признаков наличия тех или иных критических ситуаций, возникающих вследствие компьютерных атак на объекты КИС, могут использоваться различные средства обнаружения информационных угроз (далее — СОУ), к которым можно отнести широкий спектр средств мониторинга и защиты, начиная от систем физического контроля доступа и заканчивая популярными антивирусами и межсетевыми экранами. При этом каждое СОУ характеризуется вероятностью обнаружения кибератак определенного типа, а также вероятностью возникновения сигнала «ложной тревоги».

Для обеспечения максимальной степени защищенности принято использовать на объекте защиты несколько СОУ с разными принципами действия и областями контроля. В этом случае должна быть решена задача объединения показаний нескольких СОУ и принятия на их основе решения о наличии угрозы или отсутствии таковой. Объединение результатов работы СОУ возможно разными способами, обеспечивающими разную степень точности и достоверности.

Для аналогичных задач в радиотехнике наибольшее распространение получили схемы логической обработки бинарных сигналов тревоги, например, 2 из 3 ($N = 3$, $K = 2$), где N — количество независимых СОУ, K — количество поступивших сигналов об атаке. Функционирование данных схем основано на том, что число сработавших СОУ должно достигнуть и/или превысить заданную величину K, тогда формируется общий сигнал тревоги. Достоинство данного алгоритма — простота, однако отсутствие учета индивидуальных особенностей и характеристик каждого отдельно взятого СОУ не позволяет добиться наилучшего соотношения между вероятностью обнаружения и частотой генерации «ложной тревоги».

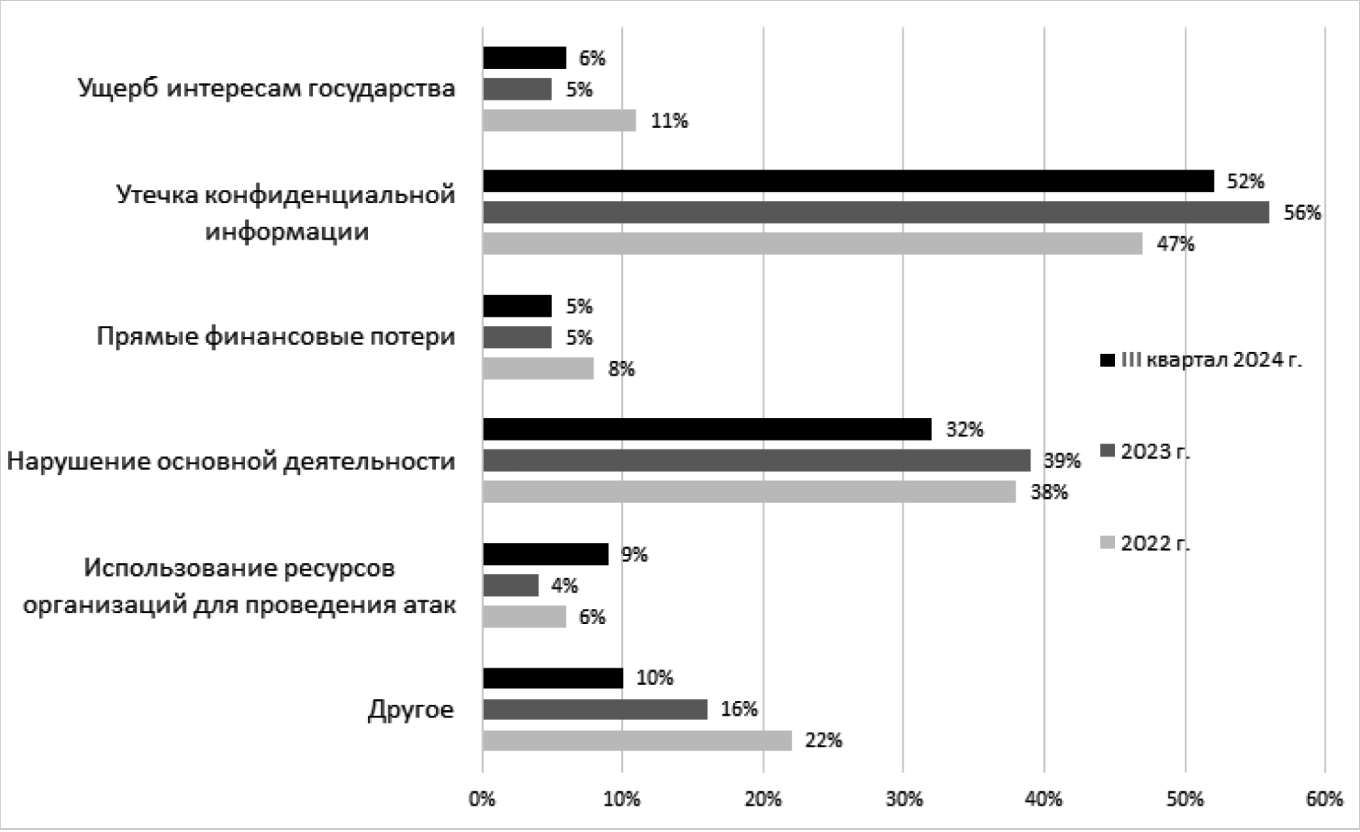

Рис. 1. Последствия атак на организации [4, 5]

Таким образом, возникает необходимость применять алгоритмы логической обработки сигналов, позволяющие за счет учета индивидуальных особенностей СОУ добиваться снижения вероятности «ложной тревоги» при сохранении заданной вероятности обнаружения.

Рассмотрим способ обнаружения информационных угроз, основанный на понятии «критической области» [6], для определения которой можно использовать метод, построенный на анализе статистических данных. Для получения необходимой информации проводится преднамеренное заражение узлов КИС различными комбинациями вирусов, осуществляется несанкционированное использование ресурсов и т.д.

Ситуацию можно трактовать так: имеется случайная величина X_0, которая принимает значение 1, если угроза обнаружена и 0 в противном случае. Экспериментатор, проводя моделирование, изменяет X_0. Средства обнаружения, позволяющие распознавать информационную угрозу, можно трактовать как X_i, где $i = 1, \ldots, n$ и n — количество СОУ. Случайные величины X_i принимают значения 0 и 1 по схеме: 1 — угроза обнаружена; 0 — угроза не обнаружена.

Итак, предметом нашего внимания является многомерная случайная величина $(X_0, X_1, \ldots, X_n)$, распределение которой мы не знаем, но стремимся изучить при помощи эксперимента.

Введем следующие обозначения:

x_0 — показатель, принимающий значения 0 или 1 (реализация X_0);

$x = (x_1, x_1, \ldots, x_n)$ — система показателей, где x_i так же принимает одно из двух значений;

K — множество всех наборов x, состоящее из $N = 2^n$ элементов;

K^* — критическая область информационных угроз (далее — КОУ), такая что если $x \in K^*$, то угроза существует, иначе угроза отсутствует, при этом $K^* \subset K$.

Эксперимент состоит из ряда наблюдений, результатом которых является статистическая функция $P = p(x_0, x_1, \ldots, x_n)$, где p — это относительная частота появления набора $(x_0, x_1, \ldots, x_n)$ в эксперименте, а сумма частот $p(x_0, x_1, \ldots, x_n)$ по всем наборам равна 1. Таким образом, выборочный закон распределения, например, случайной величины X_0 имеет вид:

X_0	0	1
вероятность	q_0	p_0

где $p_0 = \sum_{x \in K} p(1; x)$; $q_0 = 1 - p_0$. Значения величин p_0 и q_0 исследователь определяет по результатам эксперимента, и зависят от технологии его проведения.

Одним из основных является вопрос, как на основании показаний средств обнаружения X_i определить есть информационная угроза или нет. В рамках традиционного подхода он может быть решен следующим образом [6]. Пусть, например, основная гипотеза H_0 заключается в том, что угрозы нет ($X_0 = 0$), тогда H_1 — альтернативная гипотеза, означает что угроза есть ($X_0 = 1$). Тогда если $x \in K^*$, то гипотеза H_0 отвергается.

Ошибка I рода α состоит в том, что H_0 отвергается, хотя она верна, при этом α вычисляется по формуле:

$$\alpha = \frac{1}{q_0} \sum_{x \in K} * p(0; x).$$

Ошибка II рода β состоит в том, что H_0 принимается, в то время как верна H_1, и вычисляется по следующей формуле:

$$\beta = 1 - \frac{1}{p_0} \sum_{x \in K} * p(1; x).$$

Заметим, что αq_0 может быть интерпретирована как вероятность «ложной тревоги», βp_0 — как вероятность «необнаруженной информационной угрозы».

Задача состоит в том, чтобы при фиксированном уровне значимости α за счет выбора K^* минимизировать β. Она может быть решена в рамках следующего алгоритма:

Пронумеруем элементы множества K так, чтобы величины $\frac{p(1; x_a)}{p(0; x_a)}$, где $a = 1,2, \ldots, N$, не возрастали.

Построим последовательность расширяющихся подмножеств $K_a^* \subset K$, а именно: $K_0^* = \varnothing$, $K_1^* = \{x_1\}$, $K_2^* = \{x_1, x_2\}$ и т.д. Если найдутся наборы элементов x с частотой $p(0; x) = 0$, то такие наборы x включаются в подмножество K_0^*.

Далее параллельно рассчитаем две числовые последовательности:

$$0 = \alpha_0 \le \alpha_1 \le \ldots \le \alpha_{N'},$$
$$\beta_0 \ge \beta_1 \ge \ldots \ge \beta_{N'},$$

где $N' \le N$, $\alpha_a = \frac{1}{q_0} \sum_{x \in K_a^*} p(0; x)$, $\beta_a = 1 - \frac{1}{p_0} \sum_{x \in K_a^*} p(1; x)$.

На каждом шаге данного алгоритма при фиксированном уровне значимости α обеспечивается минимальность β_a, что следует из традиционного подхода [6].

При этом на каком именно шаге следует остановиться, мы решаем сами, исходя из значений α_a, β_a и выбранного нами баланса между ними. В результате экспериментатор определяет КОУ — K_a^*.

Другой подход к обнаружению информационных угроз состоит в следующем: пусть на множестве показателей K задана функция $y = f(x)$, где $x = (x_1, x_2, \ldots, x_n) \in K$, принимающая два значения 0 и 1. Таким образом мы определили разбиение K на два подмножества ($K = K_0 \cup K_1$), таких что $K_i = \{x: f(x) = i; i = 0, 1\}$.

Верно и обратное, любое такое разбиение задает функцию. Если при этом x_j принимает только два значения 0 и 1, то это булева функция. На основании имеющейся статистики $p(x_0, x)$ может быть определено выборочное распределение случайной величины $Y_f = f(x_1, x_2, \ldots, x_n)$, а именно:

Y_f	0	1
Вероятность	q_f	p_f

где $p_f = \sum_{x \in K_1} \big(p(0;x) + p(1;x)\big)$; $q_f = 1 - p_f$.

Функции f мы отводим роль «инструмента для принятия решения», а именно, если для некоторого набора показателей $x = (x_1, x_2, \ldots, x_n)$ значение $f = 1$, то принимается решение «информационная угроза есть», в противном случае «информационной угрозы нет». Таким образом, чем более коррелированы случайные величины X_0 и Y_f, тем выше качество принимаемого решения.

Для нахождения коэффициента корреляции между упомянутыми случайными величинами нужно знать их совместное распределение, которое может быть также получено из статистики $p(x_0, x)$:

X_0 / Y_f	0	1
0	p_{00}	p_{01}
1	p_{10}	p_{11}

где $p_{ij} = \sum_{x \in K_j} p(i;x)$; $i, j = 0,1..$ Величины p_{ij} связаны с ранее введенными следующими соотношениями:

$$p_0 = p_{10} + p_{11},\ q_0 = p_{00} + p_{01},\ p_f = p_{01} + p_{11},\ q_f = p_{00} + p_{10}.$$

Выборочный коэффициент корреляции между X_0 и Y_f имеет вид:

$$r_f = \frac{p_{00}p_{11} - p_{10}p_{01}}{\sqrt{p_0 q_0 p_f q_f}}.$$

Поскольку $r_{1-f} = -r_f$, то можно ограничиться рассмотрением тех функций, для которых $r_f \geq 0$ или же изучать поведение r_f^2. Задача состоит в нахождении функции f такой, что r_f принимает максимальное значение. Ее решение возможно методом перебора.

Заключение

Необходимость обеспечения информационной безопасности корпоративных информационных систем, от надежности и эффективности которых напрямую зависит конкурентоспособность организаций и предприятий, обусловлена ростом числа успешных компьютерных атак. Для обеспечения эффективной защиты объектов КИС используют различные средства обнаружения несанкционированных действий и критических ситуаций, которые обладают индивидуальными характеристиками, такими как вероятность обнаружения и вероятность генерации сигнала «ложной тревоги». Традиционные алгоритмы по объединению сигналов от множества СОУ при формировании общего решения о наличии/отсутствии угрозы не учитывают особенности каждого средства, что является их существенным недостатком.

Предложенный в работе способ объединения показаний нескольких СОУ, основанный на применении «критической области», обеспечивает оптимальное соотношение ошибок I рода и II рода, позволяя таким образом добиться оптимального соотношения значений вероятности «ложной тревоги» αq_0 и вероятности «необнаруженной информационной угрозы» βp_0. Предложенный алгоритм обнаружения киберугроз учитывает возможное взаимное влияние различных средств обнаружения друг на друга, так как в основе его работы лежит КОУ, построенная на вероятностных характеристиках общего сигнала СОУ.

ЛИТЕРАТУРА

1. Пинясова, Н.А. Конкуренция и конкурентоспособность в современной парадигме экономического развития / Н.А. Пинясова, Ю.Ю. Суслова, А.В. Волошин // Вестник Самарского государственного экономического университета. — 2024. — № 7(237). — С. 9–25.
2. Четырбок, Н.П. Инновации и конкурентоспособность предприятия / Н.П. Четырбок // Вестник Брестского государственного технического университета. — 2021. — № 2(125). — С. 123–126.
3. Как изменились атаки на российские компании за два года [Электронный ресурс] // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/kak-izmenilis-ataki-na-rossiyskie-kompanii-za-dva-goda/#id1 (Дата обращения 30.03.2025).
4. Актуальные киберугрозы для организаций: итоги 2023 года [Электронный ресурс] // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ (Дата обращения 30.03.2025).
5. Актуальные киберугрозы: III квартал 2024 года [Электронный ресурс] // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id17 (Дата обращения 30.03.2025).
6. Крамер, Г. Математические методы статистики = Mathematical Methods of Statistics: [монография] / ред. А.Н. Колмогоров; пер.: А.С. Монин, А.А. Петров; Г. Крамер. — Ижевск: Регулярная и хаотическая динамика, 2003. — 648 с.