

А.А. Нечай, С.А. Краснов, А.А. Свиначук

АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ СИСТЕМЫ ОБЩЕГО
И СРЕДНЕГО ОБРАЗОВАНИЯ

Предлагается базовая аналитическая модель обеспечения информационной безопасности образовательной организации в условиях деструктивного воздействия окружающей среды. Определены состояния, в которых может находиться моделируемая система информационной безопасности образовательной организации на определенном этапе времени.

Ключевые слова: информационная безопасность, информационные угрозы, негативные информационные воздействия, образовательная организация.

A. A. Nechai, S. A. Krasnov, A. A. Svinarchuk

ANALYTICAL MODEL FOR ENSURING INFORMATION
SECURITY OF EDUCATIONAL ORGANIZATIONS
IN THE SYSTEM OF GENERAL AND SECONDARY EDUCATION

The basic analytical model of ensuring information security of an educational organization in the conditions of destructive environmental impact is proposed. The States in which the simulated information security system of an educational organization can be located at a certain stage of time are determined.

Keywords: information security, information threats, negative information impacts, educational organization.

Введение

Информация, которая распространяется по средствам коммуникации [8], иногда имеет противоречивое содержание и негативную направленность, которая может повлиять на социально-нравственные ориентиры личности [1].

Средства массовой информации оказывают существенное влияние на окружающих. Насилие и жестокость, которые могут содержаться в информации [16], порой подаются без цензуры [5]. Особенно восприимчивы к негативной информации дети, у которых только формируются нравственные идеалы и стереотипы поведения в обществе [6]. Полностью оградить подрастающее поколение от негативной информации, которая их окружает, не получится, но научить правильно воспринимать информацию [2], ее анализировать и думать о последствиях под силу опытным учителям и педагогам [3]. В связи с этим возникает необходимость о включении в программы общего и среднего образования обучения компетенциям в области информационной безопасности (ИБ) [4].

В связи с этим на первый план выносятся задача создания безопасной информационной среды [10], которая будет благоприятно влиять на развитие личности обучающегося и формировать ее [9].

Описание модели ИБ образовательной организации (ОО)

Временные интервалы между моментами обнаружения негативных факторов [18] являются случайными [11]. Выявленные негативные информационные воздействия (НИВ) образуют поток, который близок к распределению Пуассона [12]. Временные интервалы, затраченные на обнаружение НИВ окружающей среды с требуемым признаком, также являются случайными величинами [17]. Полученные данные о признаках НИВ внешней среды [13] обрабатываются информационно-аналитической системой и после однозначной идентификации нейтрализуются по мере возможности [15]. Тем самым решается задача по нейтрализации информационных угроз (ИУ) ОО [7].

Рассмотрим случай, когда НИВ внешней среды [14] возникают с частотой, соизмеримой со временем реакции системы на идентификацию обнаруженных ИУ и их своевременную нейтрализацию системой ИБОО.

Рассмотрим всевозможные состояния, в которых может находиться моделируемая система ИБОО в определенный этап времени:

P_{00} – система обнаружения ИУ и система нейтрализации выявленных ИУ находятся в состоянии ожидания;

P_{10} – система обнаружения выявила наличие ИУ и выполняет ее идентификацию, система нейтрализации выявленных ИУ находится в состоянии покоя;

P_{01} – система обнаружения ИУ находится в состоянии покоя, а система нейтрализации выявленных ИУ занята обработкой информации о факте информационного воздействия (ИВ) и принимает меры по нейтрализации выявленной угрозы;

P_{11} – система обнаружения ИУ обнаружила факт ИВ и идентифицирует его, а система нейтрализации выявленных ИУ занята обработкой информации о факте ИВ и принимает меры по нейтрализации выявленной угрозы.

Опишем все состояния, в которых может находиться система ИБОБ, функционирующая в условиях деструктивного воздействия внешней среды.

Первое состояние. Состояние ожидания НИВ системой ИБОБ. Данное состояние возможно в следующих случаях:

- в момент времени t система обнаружения ИУ и система нейтрализации находятся в состоянии ожидания. За временной интервал Δt в области действия систем идентификации и нейтрализации не появилось ни одной угрозы. Вероятность данного факта

$$P_{00}(t)(1 - \lambda \Delta t); \quad (1)$$

- в момент времени t система идентификации и нейтрализации находилась в состоянии обработки выявленной угрозы. За время Δt данные об выявленной угрозе ИБ идентифицированы, производятся мероприятия по нейтрализации НИВ. Вероятность данного факта

$$P_{01}(t)v_2\Delta t. \quad (2)$$

Соответственно, состояние системы ИБ запишется в следующем виде:

$$P_{00}(t + \Delta t) = P_{00}(t)(1 - \lambda \Delta t) + P_{01}(t)v_2\Delta t. \quad (3)$$

После соответствующих преобразований и перехода к пределу при $\Delta t \rightarrow 0$ запишем состояние системы в виде дифференциального уравнения:

$$\frac{d}{dt}P_{00}(t) = -P_{00}(t)\lambda + P_{01}(t)v_2, \quad (4)$$

Нечай А.А., Краснов С.А., Свиначук А.А. Аналитическая модель обеспечения...

Второе состояние. Данное состояние возможно в следующих случаях:

- в момент времени t система находится в состоянии ожидания ИВ, за интервал времени Δt в области действия системы идентификации и нейтрализации не проявилось ни одного нового факта ИВ, не было нейтрализовано ни одной угрозы ИВ. Вероятность данного факта

$$P_{01}(t)(1 - \lambda\Delta t)(1 - v_2\Delta t); \quad (5)$$

- в момент времени t система ИБ находилась в режиме выявления факта ИВ, за промежуток времени Δt система ИБ передала данные о выявленном факте ИВ в систему идентификации и нейтрализации. Вероятность данного факта

$$P_{10}(t)(v_1\Delta t); \quad (6)$$

- в момент времени t система ИБ находилась в состоянии обнаружения факта ИВ и параллельно обрабатывала информацию об ИВ, а также принимала меры по нейтрализации выявленной угрозы, была полностью загружена. За интервал времени Δt система ИБ обнаружила и выдала данные о выявленном факте в систему идентификации и нейтрализации, но система ИБ эти данные не использовала, так как была занята обработкой данных о предыдущем факте ИВ. Как следствие – данные о факте ИВ, полученные от системы обнаружения, были безвозвратно потеряны вследствие кратковременности пребывания фактора в области действия системы идентификации и нейтрализации ИИВ. Вероятность данного факта

$$P_{11}(t)v_1\Delta t. \quad (7)$$

Соответственно, дифференциальное уравнение описывающее состояние системы ИБОО, запишется в следующем виде:

$$\frac{d}{dt} P_{01}(t) = -P_{01}(t)(\lambda + v_2) + P_{11}(t)v_1 + P_{10}(t)v_1. \quad (8)$$

Третье состояние. Данное состояние возможно в следующих случаях:

- в момент времени t система ИБОО находилась в состоянии покоя, за временной интервал Δt в области действия системы выявления ИУ был обнаружен факт ИИВ. Вероятность данного факта

$$P_{00}(t)\lambda\Delta t; \quad (9)$$

- в момент времени t система ИБ находилась в режиме обнаружения факта ИИВ, но информация об данном факте еще не была идентифицирована и нейтрализована; за интервал времени Δt в области действия системы обнаружения ИВ проявилось очередное ИВ, данное воздействие не было идентифицировано и нейтрализовано системой ИБ. Вероятность данного факта

$$P_{10}(t)(1 - v_1\Delta t); \quad (10)$$

- в момент времени t система ИБ была полностью загружена, был обнаружен факт ИВ, проводилась идентификация и нейтрализация выявленного факта, за интервал времени Δt источник ИИВ был идентифицирован, были приняты меры по его нейтрализации. Вероятность данного факта

$$P_{11}(t)v_2\Delta t. \quad (11)$$

Соответственно, дифференциальное уравнение для вышеописанного состояния системы ИБОО запишется в следующем виде:

$$\frac{d}{dt} P_{10}(t) = P_{00}(t)\lambda - P_{10}(t)v_1 + P_{11}(t)v_2. \quad (12)$$

Четвертое состояние. Данное состояние возможно в следующих случаях:

- в момент времени t система ИБ находилась в состоянии идентификации и нейтрализации выявленного факта ИВ, за интервал времени Δt получены новые данные об обнаруженных ИВ. Вероятность данного факта

$$P_{01}(t)\lambda\Delta t; \quad (13)$$

- в момент времени t система ИБ находилась в состоянии обнаружения, идентификации и нейтрализации выявленного факта НИВ, за временной интервал Δt не были обработаны данные по факту выявления ИВ, а в области действия защитной подсистемы появились новые факты НИВ. Вероятность данного факта

$$P_{11}(t)(1 - (v_1 + v_2)\Delta t). \quad (14)$$

Следовательно, дифференциальное уравнение для вышеописанного состояния системы ИБОО запишется в следующем виде:

$$\frac{d}{dt} P_{11}(t) = P_{01}(t)\lambda - P_{11}(t)(v_1 + v_2). \quad (15)$$

Полученная система дифференциальных уравнений, описывающая все имеющиеся состояния системы ИБОО, функционирующей в условиях негативного воздействия окружающей среды, запишется в следующем виде:

$$\begin{aligned} \frac{d}{dt} P_{00}(t) &= -P_{00}(t)\lambda + P_{01}(t)v_2; \\ \frac{d}{dt} P_{01}(t) &= -P_{01}(t)(\lambda + v_2) + P_{11}(t)v_1 + P_{10}(t)v_1; \\ \frac{d}{dt} P_{10}(t) &= P_{00}(t)\lambda - P_{10}(t)v_1 + P_{11}(t)v_2; \\ \frac{d}{dt} P_{11}(t) &= P_{01}(t)\lambda - P_{11}(t)(v_1 + v_2). \end{aligned} \quad (16)$$

Для стационарных процессов предполагаем, что переходные процессы в системе отсутствуют. Это позволяет сделать следующую запись свойств для вероятностей перехода:

$$t \rightarrow \infty, \frac{d}{dt} P_{ij}(t) \rightarrow 0, P_{ij}(t) = P_{ij} = \text{const.}$$

Тогда полученная система дифференциальных уравнений, описывающая все имеющиеся состояния системы ИБОО, преобразуется в систему алгебраических уравнений:

$$\begin{aligned} P_{00}(t)\lambda &= P_{01}(t)v_2; \\ P_{01}(t)(\lambda + v_2) &= P_{11}(t)v_1 + P_{10}(t)v_1; \\ P_{10}(t)v_1 &= P_{00}(t)\lambda + P_{11}(t)v_2; \\ P_{11}(t)(v_1 + v_2) &= P_{01}(t)\lambda, \end{aligned} \quad (17)$$

где λ – интенсивность потока НИВ; v_1 – интенсивность выявления НИВ системой ИБ; v_2 – интенсивность идентификации и нейтрализации выявленных негативных ИВ.

Система алгебраических уравнений, описывающая все возможные состояния системы ИБ:

$$\begin{aligned}
 P_{00} &= \frac{v_1 v_2}{\lambda(\lambda + v_1 + v_2) + v_1 v_2}; \\
 P_{10} &= \frac{\lambda v_2 (\lambda + v_1 + v_2)}{(v_1 + v_1)[\lambda(\lambda + v_1 + v_2) + v_1 v_2]}; \\
 P_{01} &= \frac{v_1 \lambda}{\lambda(\lambda + v_1 + v_2) + v_1 v_2}; \\
 P_{11} &= \frac{\lambda v_1}{(v_1 + v_2)[\lambda(\lambda + v_1 + v_2) + v_1 v_2]}. \tag{18}
 \end{aligned}$$

Соответственно, вероятность того, что выявленный факт НИВ будет идентифицирован и распознан системой ИБОО, составит

$$P_{\text{обс}}(t) = P_{00}(t). \tag{19}$$

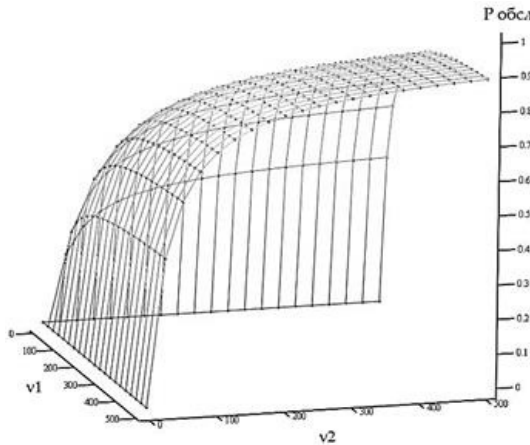
Физически процесс обнаружения, идентификации и нейтрализации фактов НИВ состоит в «прореживании» λ^* – потока негативных фактов ИВ, где λ^* – это поток негативных фактов ИВ, не обнаруженных, не идентифицированных и не нейтрализованных:

$$\lambda^* = \lambda P_{\text{отк}}, \tag{20}$$

где $P_{\text{отк}}$ – вероятность того, что факт НИВ не будет обнаружен системой ИБ.

$$P_{\text{отк}} = 1 - P_{\text{обс}}. \tag{21}$$

На рисунке изображен график зависимости вероятности обнаружения, идентификации и нейтрализации фактов ИВ от интенсивности задействования подсистем обнаружения, идентификации и нейтрализации.



Зависимость обнаружения, идентификации и нейтрализации фактов ИВ

Если проанализировать полученный график, можно увидеть, что с увеличением фактов проявления НИВ подсистемы обнаружения, идентификации и нейтрализации с такой же пропорциональностью загружаются обработкой данных фактов.

Заключение

Предложенная модель позволяет оценить эффективность работоспособности системы информационной защиты ОО, прогнозировать результаты обработки выявленных фактов ИВ и выработать определенные требования для поддержания системы ИБ образовательной организации в рамках требуемого показателя эффективности.

Литература

1. Антонович П.И., Макаренко С.И., Михайлов Р.А., Ушанев К.В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник академии военных наук. 2014. № 3 (48). С. 93–101.
2. Бубнов В.П. и др. Модели информационных систем: учебное пособие. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015. 188 с.
3. Бурлов В.Г., Грачев М.И. Модель принятия управленческих решений лица, отвечающего за информационную безопасность развития территории // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 2 (34). С. 194–198.
4. Бурлов В.Г., Лепешкин М.О. Основы модели комплексного управления процессами обеспечения техносферной безопасности региона // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 2 (34). С. 271–276.
5. Краснов С.А. О возможности смыслового анализа информации для выявления информационных интересов пользователей // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 2. С. 157–163.
6. Краснов С.А., Борисов А.А., Нечай А.А. Технология блокчейн и проблемы ее применения в различных информационных системах // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 63–67.
7. Лоскутов А.И., Дуников А.С., Артюшкин А.Б., Нечай А.А. Математическая модель системы символьной синхронизации наземной приемно-регистрирующей станции телеметрической информации в условиях флуктуаций амплитуды сигнала // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2017. Вып. 1. С. 11–19.
8. Макаренко С.И., Ковальский А.А., Краснов С.А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учеб. пособие. Ч. 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. СПб.: Научное издание технологии, 2020. 357 с.
9. Нечай А.А. Использование инновационных методов и современных технологий для повышения квалификации в области кибербезопасности // Азимут научных исследований: педагогика и психология. 2020. Т. 9, № 3 (32). С. 193–196.
10. Нечай А.А. Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий // XXIV Царскосельские чтения. 75-летие Победы в Великой Отечественной войне: материалы Международной научной конференции / под общ. ред. С.Г. Еремеева. СПб., 2020. С. 229–232.
11. Нечай А.А. Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4 (25). С. 43–44.
12. Нечай А.А., Борисов А.А., Борисова Ю.И. Точечный анализ данных дистанционного зондирования Земли средствами языка программирования Python // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 1. С. 49–55.

13. Нечай А.А., Копьев А.И. Метод управляемого распределения ресурсов между ядрами процессора // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 101–107.
14. Полончик О.Л., Артюшкин А.Б., Нечай А.А., Полончик Е.О. Радиолокационные системы дистанционного зондирования Земли на базе спутников со стабилизацией вращением // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2017. Вып. 1. С. 35–41.
15. Свиначук А.А., Нечай А.А. Использование квантовых вычислений при выборе управленческого решения // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 31–36.
16. Хомоненко А.Д., Басыров А.Г., Бубнов В.П., Забродин А.В., Краснов С.А. Модели и методы исследования информационных систем: монография / под общ. ред. А.Д. Хомоненко. СПб.: Лань, 2019. 204 с.
17. Шаймарданов А.М., Нечай А.А., Лепехин С.В. Математические модели систем автоматического управления с широтно-импульсной модуляцией // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 2. С. 27–39.
18. Эсаулов К.А., Яхваров Е.К., Нечай А.А., Березин А.С. Методика интеграции системы управления киберрисками в предпринимательских структурах // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2020. Вып. 2. С. 80–86.

Literatura

1. Antonovich P.I., Makarenko S.I., Mihajlov R.L., Ushanev K.V. Perspektivnye sposoby destruktivnogo vozdejstviya na sistemy voennogo upravleniya v edinom informacionnom prostranstve // Vestnik akademii voennyh nauk. 2014. № 3 (48). S. 93–101.
2. Bubnov V.P. i dr. Modeli informacionnyh sistem: uchebnoe posobie. M.: Uchebno-metodicheskij centr po obrazovaniju na zheleznodorozhnom transporte, 2015. 188 s.
3. Burlov V.G., Grachev M.I. Model' prinyatiya upravlencheskih reshenij lica, otvechayushchego za informacionnyuyu bezopasnost' razvitiya territorii // Informacionnye tekhnologii i sistemy: upravlenie, ekonomika, transport, pravo. 2019. № 2 (34). S. 194–198.
4. Burlov V.G., Lepeshkin M.O. Osnovy modeli kompleksnogo upravleniya processami obespecheniya tekhnosfernoj bezopasnosti regiona // Informacionnye tekhnologii i sistemy: upravlenie, ekonomika, transport, pravo. 2019. № 2 (34). S. 271–276.
5. Krasnov S.A. O vozmozhnosti smyslovogo analiza informacii dlya vyyavleniya informacionnyh interesov pol'zovatelej // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 2. S. 157–163.
6. Krasnov S.A., Borisov A.A., Nechaj A.A. Tekhnologiya blokchejn i problemy ee primeneniya v razlichnyh informacionnyh sistemah // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 63–67.
7. Loskutov A.I., Dunikov A.S., Artyushkin A.B., Nechaj A.A. Matematicheskaya model' sistemy simvol'noj sinhronizacii nazemnoj priemno-registriruyushchej stancii telemetricheskoy informacii v usloviyah fluktuacij amplitudy signala // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2017. Vyp. 1. S. 11–19.
8. Makarenko S.I., Koval'skij A.A., Krasnov S.A. Principy postroeniya i funkcionirovaniya apparatno-programmnyh sredstv telekommunikacionnyh sistem: ucheb. posobie. Ch. 2. Setevye operacionnye sistemy i principy obespecheniya informacionnoj bezopasnosti v setyah. SPb.: Naukoemkie tekhnologii, 2020. 357 s.

9. *Nechaj A.A.* Ispol'zovanie innovacionnyh metodov i sovremennyh tekhnologij dlya povysheniya kvalifikacii v oblasti kiberbezopasnosti // *Azimuth nauchnyh issledovanij: pedagogika i psihologiya*. 2020. T. 9, № 3 (32). S. 193–196.
10. *Nechaj A.A.* Kiberbezopasnost' i informacionnaya bezopasnost': sushchnost', sodержanie i otlichie ponyatij // *XXIV Carskosel'skie chteniya. 75-letie Pobedy v Velikoj Otechestvennoj vojne: materialy Mezhdunarodnoj nauchnoj konferencii / pod obshch. red. S.G. Eremeeva*. SPb., 2020. S. 229–232.
11. *Nechaj A.A.* Formirovanie bezopasnoj informacionnoj sredy // *Aktual'nye problemy sovremennosti: nauka i obshchestvo*. 2019. № 4 (25). S. 43–44.
12. *Nechaj A.A., Borisov A.A., Borisova Yu.I.* Tochechnyj analiz dannyh distancionnogo zondirovaniya Zemli sredstvami yazyka programmirovaniya Python // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2019. Vyp. 1. S. 49–55.
13. *Nechaj A.A., Kop'ev A.I.* Metod upravlyaemogo raspredeleniya resursov mezhd yadrami processora // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2018. Vyp. 2. S. 101–107.
14. *Polonchik O.L., Artyushkin A.B., Nechaj A.A., Polonchik E.O.* Radiolokacionnye sistemy distancionnogo zondirovaniya Zemli na baze sputnikov so stabilizaciej vrashcheniem // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2017. Vyp. 1. S. 35–41.
15. *Svinarchuk A.A., Nechaj A.A.* Ispol'zovanie kvantovyh vychislenij pri vybore upravlencheskogo resheniya // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2018. Vyp. 2. S. 31–36.
16. *Homonenko A.D., Basyrov A.G., Bubnov V.P., Zabrodin A.V., Krasnov S.A.* Modeli i metody issledovaniya informacionnyh sistem: monografiya / pod obshch. red. A.D. Homonenko. SPb.: Lan', 2019. 204 s.
17. *Shajmardanov A.M., Nechaj A.A., Lepekhin S.V.* Matematicheskie modeli sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyaciej // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2019. Vyp. 2. S. 27–39.
18. *Esaulov K.A., Yahvarov E.K., Nechaj A.A., Berezin A.S.* Metodika integracii sistemy upravleniya kiberriskami v predprinimatel'skih strukturah // *Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie"*. 2020. Vyp. 2. S. 80–86.