ным движением БАС и обеспечения безопасности полетов, а также для стимулирования спроса и создания условий для технологического лидерства России в этой сфере.

Цели, задачи и критерии создания ЦП БАС можно обобщить следующим образом: управление БАС и воздушным пространством, обеспечение кибербезопасности, создание условий формирования новых направлений применения и стимулирование спроса на отечественные БАС, обеспечение технологической независимости, автоматизация планирования полетов, мониторинга состояния БАС и обработки данных, сбор и обработка данных, получаемых от БАС, поддержка операций, включая правоохранительные задачи, обеспечение взаимодействия с существующими информационными системами, службами безопасности и другими платформами, безопасность и устойчивость, защита информации и данных, стимулирование инноваций, создание среды для разработки новых технологических решений, обучение и поддержка пользователей, обеспечение соответствия законодательно установленным нормам и стандартам, способствование экологически чистым решениям.

Минаев В.А.,

доктор технических наук
Московский Ордена почета университет МВД России им. В.Я. Кикотя

Эрдниев А.С.,

кандидат педагогических наук, доцент
Московский Ордена почета университет МВД России им. В.Я. Кикотя

Управление кибербезопасностью образовательного учреждения

Современная учебно-научная деятельность образовательных организаций неразрывно связана с процессами получения, хранения, обработки и передачи информации. Их информационные системы обеспечивают доступ профессорско-преподавательскому составу, сотрудникам и обучающимся к библиотекам, приложениям и сервисам, связанным с едиными базами данных. Однако, как отмечается исследователями[1], многие обеспечивающие

[1] Барабанов А.В., Марков А.С., Цирлов В.Л. Актуальные вопросы выявления уязвимостей и не декларированных возможностей в программном обеспечении // Системы высокой доступности. 2018. Т. 14. № 3. С. 12-17; Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 66-73; Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1 (9). С. 73-79; Минаев В.А., Степанов Р.О., Фаддеев А.О. Арктические риски: моделирование, комплексная оценка, управление. М.: Изд-во МГТУ им. Н. Э. Баумана, 2022. 422 с.; Щербакова Г.В. Информатизация образования

образовательные системы изначально разрабатывались без должного внимания к информационной защите, что делает их уязвимыми к кибератакам, утечкам данных и другим угрозам.

Ранжирование информационных рисков

Информационный риск рассчитывался как произведение вероятности реализации угрозы на значение возможного ущерба. В таблице 1 представлены результаты проведения экспертной оценки информационных рисков и их ранжирование для реально функционирующего образовательного учреждения.

Наибольший риск, согласно исследованию, представляют *«Сбои и отказы технических средств»* (318 баллов). Данный риск обусловлен высокой степенью зависимости научно-образовательного процесса от функционирующей техники – серверов, рабочих компьютеров, сетевого оборудования и прочих компонентов IT-инфраструктуры. Таким образом, стабильная работа технической базы является фундаментом бесперебойного функционирования вуза.

На втором месте в рейтинге наиболее опасных рисков находятся *«Ошибки специалистов по информационным технологиям»* (258 баллов). Человеческий фактор продолжает оставаться одним из самых уязвимых звеньев в системе защиты информации. Непреднамеренные действия персонала, некорректная настройка программного обеспечения, несанкционированное изменение конфигураций систем, игнорирование установленных правил безопасности, могут стать причиной серьезных инцидентов – вплоть до утечки конфиденциальных данных или повреждения их целостности.

Таблица 1

Результаты оценки информационных рисков

№	Вид информационной угрозы	Информационный риск, баллы	Ранг
1.	Сбои и отказы технических средств	318	1
2.	Ошибки IT-специалистов	258	2
3.	Сбои и отказы программных средств	222	3
4.	Сбои и отказы сетевого оборудования	195	4
5.	Вредоносное ПО	185	5
6.	Несанкционированный доступ	128	6
7.	Шпионские программы	85	7
8.	Нарушение авторских прав	62	8
9.	Аварии	45	9
10.	Пожары	24	10
11.	Другие стихийные бедствия	17	11

и проблемы кибербезопастности в образовательной среде // Современное педагогическое образование. 2020. № 11. С. 63-66.

Третье место занимают *«Сбои программных средств»* (222 балла). Проблемы, связанные с использованием устаревшего, несертифицированного или плохо совместимого программного обеспечения, увеличивают вероятность возникновения уязвимостей, которые используются злоумышленниками для совершения кибератак.

К числу угроз, характеризующихся средним уровнем риска, относятся: *«Сбои сетевого оборудования»* (195 баллов). В современном образовательном пространстве, где дистанционное обучение стало неотъемлемой частью учебного процесса, надежность сетевой инфраструктуры имеет особое значение.

«Вредоносное программное обеспечение» (185 баллов). Фишинговые атаки, использование зараженных USB-накопителей, загрузка непроверенных приложений остаются актуальными угрозами распространения вредоносного кода.

«Несанкционированный доступ к информации» (128 баллов). Опасность заключается в возможной утечке персональных данных сотрудников и студентов, а также другой конфиденциальной информации, связанной с научно-образовательной деятельностью и внутренним управлением вуза.

«Шпионские программы» (85 баллов) могут быть использованы для сбора информации о деятельности вуза, что влечет за собой потенциальный репутационный и правовой ущерб.

«Нарушение авторских прав» (62 балла) также представляет собой важный аспект, поскольку использование нелицензированного программного обеспечения или контента может повлечь административную ответственность и негативно отразиться на имидже учреждения.

«Аварии, пожары и другие стихийные бедствия» (оценка – от 17 до 45 баллов) имеют весьма низкую вероятность возникновения, однако последствия таких событий могут быть катастрофическими. Необходимо поэтому разработать и регулярно тестировать планы аварийного восстановления, а также внедрить процедуры резервного копирования и дублирования критически важных систем.

В целом исследование выявило, что технические неисправности оборудования, человеческий фактор и программные сбои составляют основу угроз информационной безопасности в вузе. Тем не менее, важно учитывать и другие угрозы, указанные в Таблице 1.

Расчет приоритетов проектов киберзащиты

Для достижения основной цели – минимизации информационных рисков – с учетом данных Таблицы 1, выделены четыре подцели: предотвращение технических сбоев и отказов, снижение ошибок персонала, защита от внешних угроз и утечек данных, минимизация последствий стихийных бедствий. А затем определены восемь проектов их достижения, по два на каждую подцель.

Далее определены эффективности каждого из проектов, путем расчета отдачи с единицы вложенных в него затрат, и проведено их упорядочивание в порядке убывания.

Пусть каждый *i*–ый проект характеризуется затратами s_i на его реализацию и ожидаемым эффектом w_i.

Обозначим через $M = \{1, 2, ..., m\}$ – множество проектов; u_i – объем затрат. Эффективность h_i проекта определим как частное от деления эффекта на затраты $h_i = w_i/u_i$.

К примеру положим, что затраты на проекты (в условных единицах) и эффекты от проектов имеют значения, показанные в таблице 2.

Сравнительную оценку эффективности проектов удобно представить графически, разместив по горизонтальной оси показатели затрат, а по вертикальной – величины ожидаемых эффектов. В результате образуется набор лучей, исходящих из начала координат. При этом эффективность проекта соответствует тангенсу угла наклона соответствующей прямой.

Таблица 2

Ранжирование проектов по эффективности

№ проекта	**Затраты на реализацию, *ui***	**Эффект, *wi***	**Эффективность, h_i**	**Затраты нарастающим итогом**	**Эффект нарастающим итогом**
3	20 000	5	0,00025	20 000	5
2	30 000	5	0,00017	50 000	10
1	50 000	7	0,00014	100 000	17
7	80 000	8	0,0001	180 000	25
5	55 000	5	0,000091	380 000	35
8	55 000	3	0,000055	435 000	40
4	200 000	10	0,00005	585 000	47
6	150 000	7	0,000047	640 000	50

Дальнейший алгоритм распределения ресурсов, согласно методике «затраты-эффект»[1], предполагает следующую последовательность действий: первоочередной реализации подлежит наиболее результативный проект, за ним – следующий по эффективности и т.д. В рассматриваемом случае порядок выполнения проектов следующий: наибольшую эффективность демон-

[1] Подр.: Модели, методы и механизмы управления научно-техническими программами : монография / В.Н. Бурков, Б.Н. Коробец, В.А. Минаев, А.В. Щепкин. М.: Изд-во МГТУ им. Н.Э. Баумана, 2017. 205 с.

стрирует третий проект, за ним следуют второй, первый, седьмой, восьмой, четвертый, пятый и завершает список шестой проект. Полученные значения эффективностей позволяют построить график «затраты – эффект», из которого, кроме последовательности выполнения проектов, видно, какой максимальный эффект может быть получен от реализации этих проектов и какие средства необходимо вложить в реализацию этих проектов. Для удобства построения графика «затраты – эффект» представим таблицу 2.

В таблице 2 представлены два столбца: кумулятивные затраты и совокупный эффект, которые отражают общий объем инвестиций и суммарный интегральный эффект. Для визуализации этих данных используется график «затраты-эффект» (рис.), построенный на основе информации из указанных столбцов таблицы. На горизонтальной оси отображаются совокупные затраты, а на вертикальной – накопленный эффект проектов. Анализ данного графика позволяет определить необходимый объем финансирования для реализации рассматриваемых проектов.

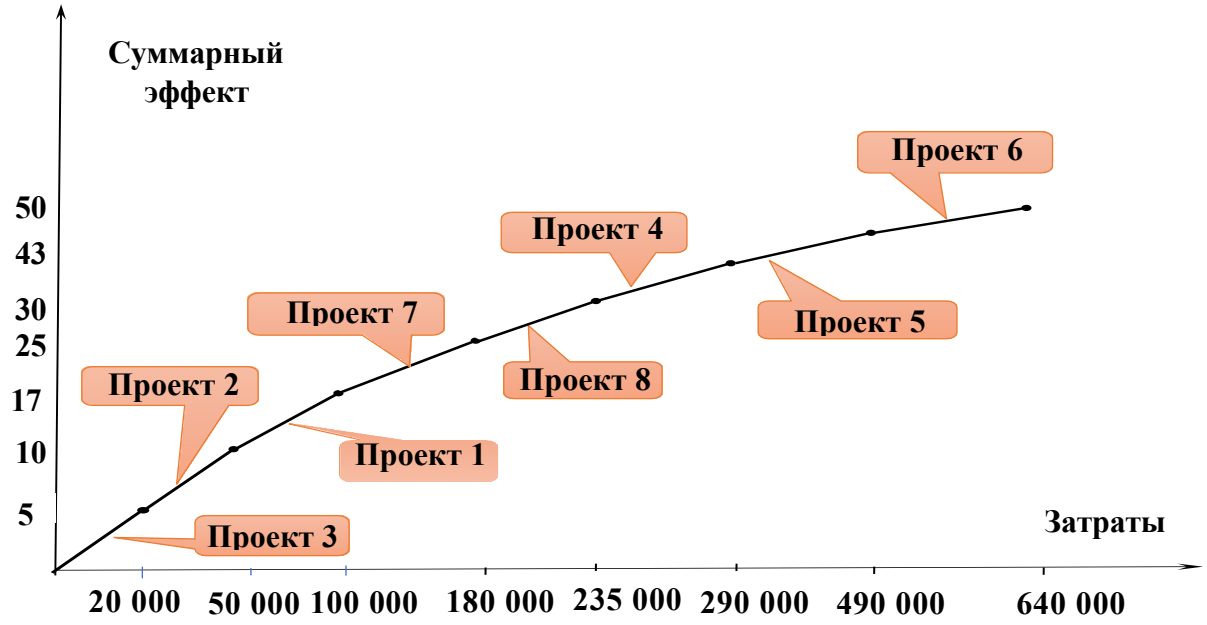

Рис. График «затраты – эффект»

Экспертный подход позволяет создавать гибкую классификацию информационных угроз, обеспечивая требуемую полноту и удобство практического использования. Формализованное табличное представление результатов позволяет выполнять автоматизированную обработку полученных результатов и получать необходимые сведения для дальнейшего управления информационными рисками.

Ранжирование – один из самых важных этапов работы при составлении карты рисков организации, после их выявления и описания. Рангом в данном случает будет являться уровень влияния конкретного риска на деятельность образовательной организации при его наступлении.

Анкетирование сотрудников и обучающихся выявило ключевые риски: сбои технических средств и ошибки персонала. Разработанная методика ранжирования проектов по эффективности (график «затраты-эффект») позволяет оптимизировать распределение ресурсов.

Углев В.А.,

кандидат технических наук, доцент
Московский Ордена почета университет МВД России им. В.Я. Кикотя

Искусственный интеллект: нормативно-правовая база

Средства специальной робототехники и искусственного интеллекта стали неотъемлемой часть работы специальных служб, включая подразделения Министерства внутренних дел. Сегодня никого не удивишь роботом для разминирования, дроном, умными камерами и системами распознавания лиц на вокзалах и в аэропортах. Если система не управляется напрямую человеком-оператором, то в дело вступает искусственный интеллект (ИИ).

Для регулирования применения ИИ на территории Российской Федерации существуют ряд нормативных документов. Если до появления национальной стратегии развития ИИ на период до 2030 года (Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» с последующей редакцией от 15.02.2024 № 124) в этой области в основном применялись нормативные документы по программной инженерии, то с 2019 года встал вопрос о формировании нового стека стандартов.

Обращаясь к материалам Росстандарта (Федерального агентства по техническому регулированию и метрологии), можно выяснить, что в области ИИ приняты и действуют 102 государственных стандарта (ГОСТа) и 50 предварительных национальных стандартов (ПНСТ). Некоторые из них, имея статус ISO, используют в основе зарубежные стандарты. В целом с 2019 года проделана большая работа по документированию технологий в этой области (рис. 1).

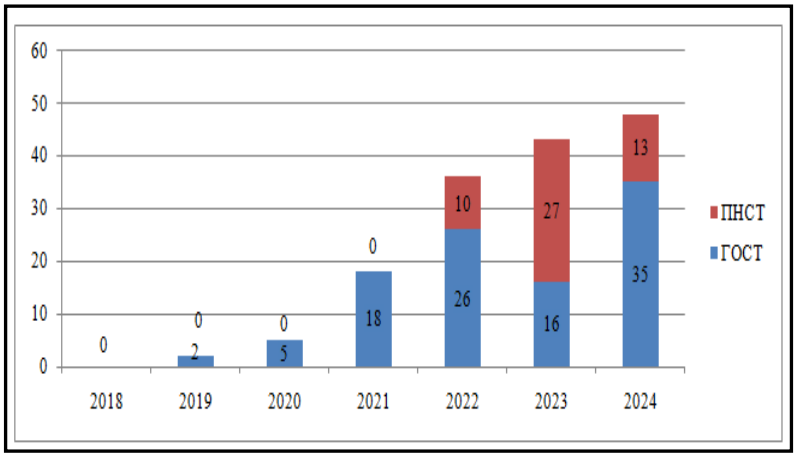

Рис. 1. Число принятых/обновленных стандартов Российской Федерации в области ИИ с 2018 г.