Российский экономический интернет-журнал №1/2023
Научная статья
Original article
УДК 330.34

Концепция средств защиты на основе применения искусственного интеллекта для обеспечения кибербезопасности государства

Чугунов В.В., магистрант 2 курса направления подготовки «Государственное и муниципальное управление»
Обнинский институт атомной энергетики – филиал Национального исследовательского ядерного университета «МИФИ» , Обнинск, Россия
Найденкова К.В., к.э.н., доцент отделения социально-экономических наук
Обнинский институт атомной энергетики – филиал Национального исследовательского ядерного университета «МИФИ», Обнинск, Россия

Аннотация. Научная статья раскрывает такую важную и актуальную на сегодняшний день тему, как использование технологий искусственного интеллекта в области кибербезопасности. Проанализированы основные направления защиты информации, в которые активно интегрируются модули искусственного интеллекта. Предложена концепция средств защиты с применением искусственного интеллекта на базе существующего отечественного ПО, в том числе с целью обеспечения технологической независимости РФ. На основе экспертного опроса подтверждена практическая значимость и целесообразность внедрения в различных отраслях экономики систем защиты на базе технологий искусственного интеллекта.

Ключевые слова: искусственный интеллект, кибербезопасность, кибератака

The concept of protective equipment based on the use of artificial intelligence to ensure the cybersecurity of the state

Chugunov V.V., student of master's program for «State and municipal management»

Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia
Naydyonkova K.V., Candidate of Economic Sciences, associate professor of Department of social and economic sciences
Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia

Annotation. The scientific article reveals such an important and relevant topic as the use of artificial intelligence technologies in the field of cybersecurity. The main directions of information protection, in which artificial intelligence modules are actively integrated, are analyzed. The concept of means of protection with the use of artificial intelligence on the basis of existing domestic software is proposed, in order to increase its effectiveness and ensure the technological independence of the Russian Federation. Based on a survey of 25 employees of the information security departments of enterprises and organizations of the Kaluga region, the practical significance and expediency of introducing protection systems based on artificial intelligence technologies in various sectors of the economy were confirmed.

Key words: artificial intelligence, cybersecurity, cyberattack

В настоящее время единственным отечественным производителем ПО для обеспечения кибербезопасности в России, который использует технологии искусственного интеллекта (ИИ), является Лаборатория Касперского, производящая средства для обнаружения вредоносных программ. Несмотря на их высокую эффективность в сегменте частных решений для защиты домашних устройств, их функционала зачастую недостаточно для борьбы с серьезными кибератаками из-за многоаспектности атак и отсутствия предиктивных механизмов защиты для предотвращения вторжений.

Проведенный нами анализ механизмов обеспечения кибербезопасности в организациях различной отраслевой принадлежности показал, что представленные на рынке отечественные решения в основном отличаются фрагментарностью: они способны эффективно противодействовать определенным типам киберугроз, но не всему их многообразию, что не позволяет создать на их основе полноценный контур защиты киберпространства организации. По этой причине

большинство крупных российских предприятий на протяжении многих лет активно использовали защитное ПО для предотвращения кибератак и мониторинга безопасности на основе искусственного интеллекта зарубежного производства, т.к. отличительной особенностью зарубежных решений была высокая эффективность обнаружения и блокирования угроз «нулевого дня» - угроз, против которых ещё не разработаны защитные механизмы [1]. Поставщиками данного ПО являлись такие компании, как: Symantec, IBM, Cylance, Cisco и другие.

В феврале-марте 2022 года в связи с началом проведения Россией специальной военной операции все иностранные производители ПО объявили о своём уходе с российского рынка, а также прекратили его поддержку. Дальнейшее использование зарубежного ПО становится гораздо менее эффективным из-за невозможности его актуализации, а также небезопасным, так как все страны-разработчики данного ПО являются недружественными по отношению к РФ и могут модернизировать методы кибератак для обхода своих же программных средств защиты. Также на основании Указа Президента РФ от 30.03.2022 №166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» с 1 января 2025 года данное ПО будет запрещено для использования на объектах критических информационных инфраструктур (КИИ) [4, 5].

В связи с данными обстоятельствами, Российская Федерация нуждается в разработке собственного комплекса средств защиты информации, в основе функционирования которого будет заложен искусственный интеллект.

Необходимость применения искусственного интеллекта в средствах защиты информации обусловлена следующими причинами:

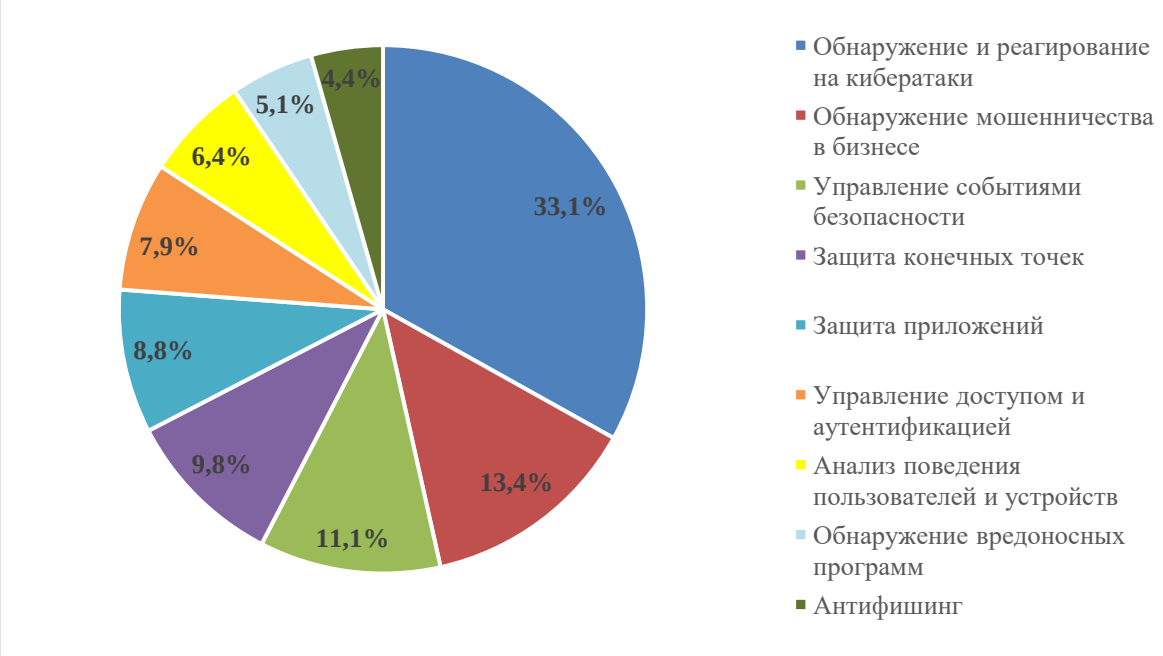
1) дефицит специалистов в области кибербезопасности;

2) существенно увеличившийся в последние годы объем данных, обрабатываемый устройствами;

3) увеличение количества кибератак за в марте-сентябре 2022 г. в 11 раз по сравнению с аналогичным периодом 2021 г.;

4) использование технологий ИИ злоумышленниками, способных обходить средства защиты без использования ИИ.

Существует 9 основных направлений средств защиты информации с применением технологий ИИ, которые отличаются по сценариям использования, а также по функциональному типу. На рис. 1 представлены все существующие направления защиты и их доля от общего числа продуктов с применением технологий ИИ на глобальном рынке кибербезопасности.



Источник: [3]

Рис. 1 – Распределение продуктов с применением технологий ИИ в области кибербезопасности по сценариям использования

По данным рис. 1 можно наблюдать значительный перевес доли средств обнаружения и реагирования на кибератаки, которые составляют почти треть от общего числа средств защиты с применением ИИ, в то время как средства обнаружения вредоносных программ (антивирусы) и средства антифишинга, которые ещё несколько лет назад лидировали на рынке кибербезопасности и являлись самыми востребованными направлениями защиты, сейчас в совокупности составляют менее 10% от общей доли рынка. Данная статистика подтверждает высокую скорость развития и изменения трендов кибербезопасности и необходимость использования инновационных технологий в её защите.

Использование всех имеющихся разновидностей средств защиты предоставит возможность быть защищенным от простых до самых сложных атак, однако стоимость необходимого технического оборудования для их обслуживания может быть слишком велика для многих объектов КИИ, для которых данный комплекс средств необходим в первую очередь, поэтому в предлагаемом комплексе средств должны использоваться такие направления защиты, которые подойдут большинству организаций как в государственном секторе, так и в коммерческом.

Например, системы выявления и предотвращения мошеннических операций и угроз в бизнес-процессах очень полезны для коммерческих предприятий, но для государственных учреждений и большинства объектов КИИ их использование нецелесообразно ввиду малого количества или отсутствия самих бизнес-процессов в их деятельности.

Приоритетным направлением в предполагаемом комплексе средств защиты будет являться система обнаружения и реагирования на кибератаки NDR (Network Detection and Response). Её главной задачей является обнаружение атак в сетевом периметре и оперативное реагирование на них. Необходимость использования данной системы подтверждается ее популярностью на глобальном рынке ИИ, которая составляет 33,1% от общего числа систем защиты.

Принцип работы данной системы заключается в использовании сформированных и регулярно обновляемых баз данных статистики и угроз, непрерывно анализируемых искусственным интеллектом с помощью технологий глубинного обучения. В результате анализа этих данных система заблаговременно определяет угрозы в сетевом периметре и может автоматически на них реагировать надлежащим образом, изменяя конфигурацию сетевых устройств и шлюзов.

Главным отличием от аналогичных средств защиты без применения ИИ является возможность построения модели потенциальных угроз, с помощью которой можно блокировать даже те атаки, алгоритм которых ещё не известен базам данных [2]. Это в первую очередь необходимо для отражения кибератак, в которых также используется ИИ, ведь именно с его помощью хакеры обходят

существующие системы защиты при помощи скорости видоизменения вредоносных файлов и сценария атаки в реальном времени.

Дополнительной функцией данной системы является анализ почтового трафика на предмет фишинга, что освобождает от потребности в использовании отдельной системы по защите от него. По данным исследований Института информационных технологий Capgemini, 89% организаций, которые применяли технологии ИИ в системах обнаружения и реагирования на кибератаки, заявляют о сокращении времени реагирования и снижении затрат на их обнаружение и предотвращение. Статистические показатели эффективности ИИ в системах обнаружения и реагирования на кибератаки на организации приведены в табл. 1.

Таблица 1

Статистика сокращения расходов на детектирование и реагирование на кибератаки при использовании технологий ИИ

Показатели	**Процент организаций, сообщивших об улучшении показателя:**	
	На 1-20%	**Более чем на 20%**
Сокращение стоимости обнаружения уязвимостей	54	29
Сокращение стоимости восстановления IT-системы от случившихся кибератак	51	19
Сокращение времени обнаружения уязвимостей	53	35
Сокращение времени нейтрализации кибератак	65	20

Вторым направлением в предлагаемом комплексе средств защиты информации целесообразно выбрать систему управления событиями безопасности SIEM (Security Information and Event Management). Основной задачей данного направления защиты является мониторинг информационных систем, анализ событий безопасности в режиме реального времени, исходящих от сетевого оборудования, систем защиты информации и сетевой инфраструктуры, IT-сервисов и приложений, которые в свою очередь помогают обнаружить инциденты информационной безопасности. Основным преимуществом применения технологий ИИ в данной системе является возможность обнаружения аномального

поведения и сокращения ложных срабатываний при изменении шаблонов и моделей данных.

Основной проблемой SIEM-систем является сильная зависимость от экспертов по работе с данными систем ввиду их сложности, а также их огромного объема, который эксперты не успевают обработать. По данным технологического института Escal, применение искусственного интеллекта в SIEM-системах позволяет достигнуть очень высокого уровня автоматизации и нивелирует потребность в расширении штата специалистов по информационной безопасности [6].

Третьим направлением стоит выбрать не самую популярную на мировом рынке, но очень востребованную систему поведенческого анализа пользователей и информационных сущностей UEBA (User and Entity Behavior Analytics). Её задачей является обнаружение случаев необычного поведения в целях обнаружения внешних и внутренних угроз. Технологии искусственного интеллекта в данном виде систем помогают автоматически выявлять аномалии в моделях поведения пользователей (отклонение от нормы или соответствие шаблону (паттерну) угрозы) для различных элементов информационных систем.

Выявленные аномалии идентифицируются искусственным интеллектом как различные угрозы и риски для бизнеса. Выявление аномального поведения может применяться в целях мониторинга и управления доступом, обнаружения мошенничества среди клиентов или сотрудников, защиты персональных данных, проверки соблюдения тех или иных регламентов и нормативных актов. Системы UEBA упрощают работу сотрудникам по безопасности путём автоматического решения множества задач, опираясь на сформированные модели поведения пользователей и других элементов информационных систем, с последующим выявлением «белых ворон», тем самым определяя:

- неавторизованный доступ и перемещение данных;
- подозрительное поведение привилегированных пользователей;
- вредоносную активность сотрудников;
- нестандартный доступ и использование облачных ресурсов.

Если говорить о применении технологий ИИ в защите кибербезопасности в целом, без привязки к конкретному сценарию защиты, то по данным опроса консалтинговой компании в области кибербезопасности Osterman Research, охватывавшего более 100 организаций, относящихся к сфере среднего и крупного бизнеса и осуществляющих деятельность в различных отраслях промышленности и сферы услуг, 81% компаний, которые начали использовать ПО разных сценариев защиты с применением технологий ИИ, отмечают повышение эффективности в расследовании инцидентов, обнаружения и скорости реакции на угрозы. Многие респонденты также обращают внимание на сокращение количества ложных срабатываний. Более подробная статистика по улучшению показателей безопасности представлена в табл. 2.

Таблица 2

Статистика по улучшению показателей информационной безопасности после применения технологий ИИ, %

Преимущества	**Все организации**	**Организации с долей применения ИИ менее 10%**	**Организации с долей применения ИИ 10% и более**
Быстрота обнаружения угроз	60	47	71
Увеличение эффективности деятельности отделов по безопасности	59	45	70
Автоматизация сортировки данных	47	39	53
Оптимизация обнаружения угроз	46	42	52
Сокращение числа ложных срабатываний	37	26	51
Автоматическое восстановление системы после кибератаки	22	16	29

Как видно из данных табл. 2, даже организации, относительно слабо использующие ИИ в собственной системе информационной безопасности, отмечают достаточно существенные улучшения от его применения для обнаружения различных типов угроз. В то же время, в организациях с более высокой долей применения технологий ИИ фиксируется практически 2-кратное улучшение значения параметра «Автоматическое восстановление системы после кибератаки»,

существенный рост эффективности наблюдается и по параметрам «Быстрота обнаружения угроз» и «Сокращение числа ложных срабатываний». Как показывают статистические данные, организации, активно применяющие технологии ИИ обеспечения защиты от киберугроз, более адекватно могут на их основе выстроить текущую деятельность отделов по безопасности и повысить эффективность автоматизации сортировки данных.

Для оценки целесообразности и эффективности внедрения ИИ в обеспечение кибербезопасности, а также выявления наиболее востребованных систем защиты, был проведен опрос 25 сотрудников, работающих с сетевой инфраструктурой и обеспечением её защищенности в организациях различной направленности Калужской области. В табл. 3 представлен перечень вопросов и возможные варианты ответа.

Таблица 3

Перечень вопросов и вариантов ответа для сотрудников отделов информационной безопасности

№ вопроса	Вопрос	Варианты ответа
1	С каким количеством инцидентов информационной безопасности в месяц вы сталкиваетесь?	1) 0-1 2) 2-5 3) 6-10 4) Больше 10
2	Сколько из вышеперечисленных инцидентов приходится на кибератаки?	1) 0-25% 2) 26-50% 3) 51-75% 4) 76-100%
3	Используете ли вы средства защиты безопасности кроме антивируса?	1) Да 2) Нет
4	Если в 3 вопросе вы ответили «нет», считаете ли вы эту меру безопасности достаточной?	1) Да 2) Нет
5	Какой процент кибератак удается предотвратить до того момента, как они наносят ущерб?	1) 0-25% 2) 26-50% 3) 51-75% 4) 76-100%
6	По шкале от 1 до 10, насколько защищенной вы считаете свою сетевую инфраструктуру от нынешних угроз?	1 – абсолютно не защищена, 10 – абсолютно защищена
7	Необходимы ли вам дополнительные сотрудники для более эффективного противодействия текущим проблемам?	1) Да, необходимо значительное расширение штата

		2) Да, нужен 1 или 2 дополнительных сотрудника 3) Нет необходимости
8	Могут ли, по вашему мнению, более продвинутые средства защиты с применением технологий ИИ помочь вам в решении текущих проблем?	1) Да 2) Нет 3) Затрудняюсь ответить
9	Начиная с 24 февраля 2022 года, заметили ли вы значительное увеличение числа кибератак на вашу организацию?	1) Да 2) Нет
10	По шкале от 1 до 10, насколько необходимо приобретение дополнительного программного обеспечения и оборудования для его функционирования в целях более эффективного противодействия текущим проблемам?	1 – нет необходимости, 10 – критически необходимо

Источник: собственная разработка

Результаты данного опроса отображены в табл. 4.

По результатам данного опроса можно сделать следующие выводы: 92% опрошенных отметили, что сталкиваются в среднем с 8 и более инцидентами информационной безопасности в месяц. Инцидент информационной безопасности, согласно мнению респондентов, – это появление одного или нескольких нежелательных, или неожиданных событий, с которыми связана значительная вероятность компрометации и создания угрозы для структуры безопасности всей организации.

Согласно результатам обработки ответов респондентов, в 79,5% случаев причиной возникновения данных инцидентов становятся кибератаки, а не человеческий фактор (посещение подозрительных сайтов, несоблюдение политики информационной безопасности организации и т.д.), при этом 76% организаций в качестве средства защиты используют только антивирусы, основной целью которых является защита именно от инцидентов, связанных с человеческим фактором.

72% специалистов отметили, что использования одного антивируса недостаточно. Предотвратить ущерб получается в среднем лишь от 45,5% атак, остальные 54,5% атак в той или иной степени становятся помехой для рабочего процесса всей организации.

Таблица 4

Результаты проведенного опроса в отношении моделей обеспечения информационной и кибербезопасности

№ вопроса	Вариант ответа и частота его выбора, %				
1	0-1	2-5	6-10	Больше 10	
	0	8	52	40	
2	0-25%	26-50%	51-75%	76-100%	
	0	4	24	72	
3	Да	Нет			
	24	76			
4	Да	Нет			
	28	72			
5	0-25%	26-50%	51-75%	76-100%	
	20	44	24	12	
6	1-2	3-4	5-6	7-8	9-10
	4	12	28	8	4
7	Да, необходимо значительное расширение штата	Да, нужен 1 или 2 дополнительных сотрудника	Нет необходимости		
	88	12	0		
8	Да	Нет	Затрудняюсь ответить		
	80	0	20		
9	Да	Нет			
	96	4			
10	1-2	3-4	5-6	7-8	9-10
	0	12	24	34	30

Источник: собственная разработка

Примечательна статистика по шестому вопросу: 44% сотрудников затруднились дать ответ на данный вопрос, т.к. не обладают достаточными компетенциями или не могут охватить всю инфраструктуру организации. Преимущественно эти сотрудники работают в больших организациях, в которых функционирует более 10 серверов и более 100 ПЭВМ. Данный факт говорит о необходимости проведения IT-аудита крупных организаций. Отметим, что подобная проблема характерна для всех без исключения регионов и организаций различной отраслевой и ведомственной принадлежности.

100% сотрудников сочли необходимым расширение штата безопасности, при этом 88% нуждаются в значительном расширении штата, что также говорит о необходимости использования ИИ, который упростит рутинную работу

сотрудников отделов информационной безопасности. Также 100% сотрудников, знакомых с технологиями ИИ, согласны с их эффективностью и целесообразностью их применения. 80% от всех опрошенных сотрудников считает в той или иной степени необходимым усиление имеющихся мер защиты и применение в них технологий ИИ. Из вышеперечисленных статистических данных можно также сделать вывод о целесообразности внедрения ИИ в процесс работы организаций различного профиля.

Таким образом, с учётом отсутствия вышеперечисленных направлений защиты на российском рынке, ухода иностранных производителей и невозможности зависимости от предлагаемых ими решений ввиду их потенциальной угрозы использования в целях шпионажа, а также по приведенной статистике улучшения ключевых показателей защищенности предприятий от кибератак, мы можем сделать вывод о перспективности и целесообразности с технической точки зрения создания комплекса средств защиты с применением искусственного интеллекта на базе отечественных программных решений.

Библиографический список:

1 Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество, политика, экономика, право. – 2017. – № 3. – С. 28-32.

2 Минбалеев А.В. Проблемы использования искусственного интеллекта в противодействии киберпреступности / [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-iskusstvennogo-intellekta-v-protivodeystvii-kiberprestupnosti/viewer (дата обращения: 09.11.2022).

3 Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность / [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost/viewer (дата обращения: 18.09.2022).

4 Официальное интернет-представительство Президента России [Электронный ресурс] Режим доступа: http://www.kremlin.ru (дата обращения: 13.11.2022).

5 Официальный сайт национального провайдера технологий кибербезопасности Ростелеком-Солар [Электронный ресурс] Режим доступа: https://rt-solar.ru/ (дата обращения: 21.10.2022).

6 Сафонова М.Ф., Ципляева С.А.: Кибербезопасность: Проблемы и решения / [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-problemy-i-resheniya/viewer (дата обращения: 21.09.2022).

References:

1 Bulavin A.V. On the approaches of the USA and China to ensuring cyberbullying // Society, politics, economics, law. - 2017. – № 3. – pp. 28-32.

2 Minbaleev A.V. Problems of using artificial intelligence in countering cybercrime / [Electronic resource] Access mode: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-iskusstvennogo-intellekta-v-protivodeystvii-kiberprestupnosti/viewer (date of application: 09.11.2022).

3 Namiot D.E., Ilyushin E.A., Chizhov I.V. Artificial intelligence and cybersecurity / [Electronic resource] Access mode: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost/viewer (accessed: 09/18/2022).

4 Official Internet representation of the President of Russia [Electronic resource] Access mode: http://www.kremlin.ru (accessed: 13.11.2022).

5 Official website of the National provider of cybersecurity technologies Rostelecom-Solar [Electronic resource] Access mode: https://rt-solar.ru / (accessed: 10/21/2022).

6 Safonova M.F., Tsiplyaeva S.A.: Cybersecurity: Problems and solutions / [Electronic resource] Access mode: https://cyberleninka.ru/article/n / kiberbezopasnost-problem-i-resheniya/viewer (accessed: 09/21/2022).

Для цитирования: Чугунов В.В., Концепция средств защиты на основе применения искусственного интеллекта для обеспечения кибербезопасности государства / Чугунов В.В., Найденкова К.В. // Российский экономический интернет-журнал. – 2023. – № 1. URL: