Направления интеллектуализации систем безопасности

Directions of intellectualization of security systems

УДК 681.322
Получено: 19.02.2022 Одобрено: 06.03.2022 Опубликовано: 25.03.2022

Гарькушев А.Ю.
Канд. техн. наук, профессор кафедры обеспечения служебно-боевой деятельности войск национальной гвардии Российской Федерации. Санкт-Петербургский военный институт войск национальной гвардии.
e-mail: sangark@mail.ru.

Garkushev A.Yu.
Candidate of Technical Sciences, Professor of the Department for Support of Service and Combat Activities of the National Guard Troops of the Russian Federation. St. Petersburg Military Institute of the National Guard Troops.

Курилов А.В.
Начальник кафедры обеспечения служебно-боевой деятельности войск национальной гвардии Российской Федерации. Санкт-Петербургский военный институт войск национальной гвардии.
e-mail: AK1225@rambler.ru

Kurilov A.V.
Head of the Department for Support of Service and Combat Activities of the National Guard Troops of the Russian Federation. St. Petersburg Military Institute of the National Guard Troops.

Сысуев С.Ю.
Канд. военных наук, доцент, Михайловская Военная артиллерийская академия, г. Санкт-Петербург.
e-mail: sysuev1971@mail.ru.

Sysuev S.Yu.
Candidate of Military Sciences, Associate Professor, Mikhailovskaya Military Artillery Academy, St. Petersburg.

Кастырин М.А.
Аспирант, Российский университет дружбы народов, кафедра таможенного дела.

Kastyrin M.A.
Postgraduate student, Peoples' Friendship University of Russia, Department of Customs.

Аннотация
Статья посвящена анализу возможностей искусственного интеллекта по парированию угроз кибербезопасности информационных управляющих систем на различных объектах. Выявлены основные направления реализации угроз цифровой безопасности, основные нарушители режима и возможные способы парирования опасностей со стороны

информационного обмена и программного обеспечения комплексов инженерно-технических средств охраны.
Ключевые слова: информационная угроза, опасность, нарушитель.

Abstract
The article is devoted to analyzing the capabilities of artificial intelligence in parading cybersecurity threats of information control systems at various facilities. The main directions of implementation of digital security threats, the main violators of the mode and possible ways of preventing hazards from the information exchange and software of security engineering and technical systems have been identified.
Keywords: information threat, danger, violator.

Развитие систем обеспечения безопасности промышленных предприятий, объектов транспортной инфраструктуры и коммерческих объектов техническими средствами [1-3], которые обеспечивают основные функции недопущения несанкционированного воздействия на объект защиты, разрешает целый круг проблем, связанных, прежде всего, с нейтрализацией негативного влияния человеческого фактора на общую безопасность объекта. Современные системы безопасности уже успешно решают такие прикладные задачи как [4-9]:

- повышение безопасности объектов за счет интеллектуализации (автоматизации) компьютерных процессов принятия решения с исключением человеческого фактора; обнаружение на объекте угрозы безопасности, актов незаконного вмешательства и эпизодов несанкционированного доступа на объект: нахождение людей и / или технических средств в том числе роботизированных в той области объекта, в которой их нахождение не предусмотрено;
- наблюдение за объектовой посещаемостью, временем пребывания на объекте посетителей, их текущим положением и присутствием на объекте в особые периоды (ночь, в выходные и праздники, в нерабочее время, время ремонта и т.д.) - подсчёт людей и технических средств, появляющихся и покидающих территорию объекта;
- получение информации о людях, посещающих объект – распознавание известных системе людей, фиксация неизвестных;
- определение факта проникновения на объект беспилотных воздушных, наземных и водных роботизированных аппаратов;
- активация внешних относительно системы устройств (например, устройств управления доступом, устройств оповещения и т.д.) в зависимости от происходящих на объекте событий;
- наблюдение за функциональным состоянием должностных лиц (охранников);
- построение индивидуальных траекторий перемещений посетителя внутри объекта в зависимости от его статуса, обеспечение индивидуальной навигации внутри объекта.

Часто для отображения информации используется интерфейс пользователя, включая мобильные устройства (смартфоны, планшеты). Именно здесь злоумышленники будут пытаться найти брешь в защите информационного поля систем безопасности. Как правило, они стараются реализовать свои замыслы, воздействуя на различные элементы, связанные с контролем доступа на объект через единое информационное поле [10, 11]. При этом направленность угроз (рис. 1) связана либо с модификацией средств защиты, либо с воздействием непосредственно на устройства контроля доступа, а также с подменой или внедрением вирусных элементов в программное обеспечение защитной системы [12-18].

Рис. 1. Возможные бреши в безопасности различных объектов

]Как наглядно показано на рис. 1, нарушитель может попытаться подделать личную карточку с магнитным или RFID идентификатором, нарушить кодировку приемо-передающего устройства (считывателя или сканера) на турникете или шлагбауме. Кроме того, существует угроза применения «администраторского» ключа, который используется в тестовых и ремонтных целях и может непосредственно воздействовать на электронную часть запорных механизмов, а также подменять «отклик» считывателей, пересылаемый в единую информационную систему.

Другим направлением сосредоточения усилий нарушителей является удаленная работа с программными средствами [19-21]. Прежде всего это создание таких программ, которые позволяют обойти различные программные закладки в базовой платформе и имитировать нормальную работу системы при ее взломе или выведению из строя другим способом, например, вирусной атакой. Модификацией этого метода является внедрение в управляющие контуры программ или механизмов, парализующих действие системы контроля удаленного доступа (СКУД). В этом случае оператор СКУД может принять решение об аварийном отключении системы и переходе на ручную проверку лиц, пересекающих границы объекта. Именно в переходный период возможны попытки проникновения на объект.

К числу основных методов, охватывающих все уровни представления информации, при реализации угроз информационной безопасности относятся [22-24]:

– определение злоумышленником типа и параметров носителей информации и· получение информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

– получение злоумышленником детальной информации о функциях, выполняемых системой и данных о применяемых системах защиты;

– определение способа представления информации и содержания данных, обрабатываемых в системе, на качественном уровне (применяется для мониторинга и для дешифрования сообщений);

– хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные и· уничтожение средств вычислительной техники и носителей информации;

– использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) и перехват данных, передаваемых по каналам связи, а также уничтожение носителей информации, а также внесение пользователем несанкционированных изменений в программно-аппаратные компоненты системы и обрабатываемые данные;

– несанкционированный доступ пользователя к ресурсам системы в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов и· превышение пользователем своих полномочий и· несанкционированное копирование программного обеспечения;

– раскрытие представления информации (дешифрование данных) и· раскрытие содержания информации на семантическом уровне;

– установка и использование нештатного аппаратного и / или программного обеспечения;

– заражение программными вирусами и целенаправленное внедрение дезинформации, а также искажение соответствия синтаксических и семантических конструкций языка;

– выведение из строя носителей информации без уничтожения;

– проявление ошибок проектирования и разработки аппаратных и программных компонентов.

Для своевременного парирования перечисленных угроз необходимо применять комплексирование мультисенсорных данных, полученных от системы технического (компьютерного) зрения и от охранных датчиков. Сигналы от охранных датчиков представляют собой разреженный и малоинформативный, но относительно достоверный поток информации, а системы видеонаблюдения (в том числе и использующие технологии компьютерного зрения) наоборот выдают, как правило, избыточную и не всегда однозначно интерпретируемую информацию (избыточный, но информативный поток данных). Комплексирование этих потоков данных позволяет, с одной стороны, сохранить высокую информативность видеопотока, а с другой — упростить и ускорить для пользователя переход к важным для него ситуационным и временным фрагментам этого потока.

В настоящее время еще ни в одной системе не применяется полноценно семантический анализ полученных данных, что не позволяет представить полученные и обработанные системой данные в виде инфографических символов или текста, понятного конечному пользователю. Такое представление информации могло бы существенно упростить навигацию по массиву данных, поиск интересующих пользователя событий, а также сделает возможным статистический анализ полученного массива данных. Кроме того, это привело бы к сокращению времени на уяснение обстановки, а, следовательно, повышению оперативности принимаемых решений, а также обеспечило интеллектуальному блоку поддержки принятия решений возможность генерировать их более качественные варианты. Это, в свою очередь, значительно повысит обоснованность принимаемых решений по реагированию на угрозы безопасности объекта.

Анализ взаимосвязи функций систем безопасности и способов их реализации показывает, что максимальный информационный обмен приходится на предотвращение несанкционированного доступа на объект. Это приводит к тому, что редкие события часто оказываются вне зоны усиленного наблюдения и угрозы от них своевременно не купируются [25-27].

Основные угрозы, по мнению специалистов [28-31], исходят не только от внешних злоумышленников, но и от персонала предприятия (учреждения). Практика показывает, что на долю внутренних нарушителей приходится более 2/3 от общего числа нарушений.

При этом можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

Внутренним нарушителем может быть лицо из следующих категорий персонала (рис. 2):

– руководители различных уровней должностной иерархии;

– пользователи системы;

– сотрудники отделов разработки и сопровождения программного обеспечения и · персонал, обслуживающий технические средства;

– технический персонал, обслуживающий здания (уборщики, электрики, сантехники и др.);

– сотрудники службы безопасности.

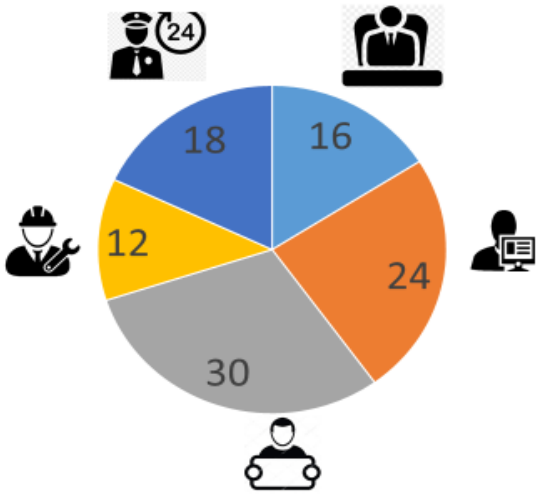

Рис. 2. Типовое процентное распределение нарушений по категориям сотрудников

Предотвращение актов незаконного вмешательства в деятельность объекта защиты осуществляется обоснованным и своевременным применением комплекса мер парирования угроз информационной безопасности [32, 33] (рис. 3).

Рис. 3. Средства обеспечения кибербезопасности.

Целесообразно строить автономную систему кибербезопасности в составе:

- подсистема приёма и начальной обработки видеоинформации;
- подсистема приёма сигналов от охранных датчиков;
- подсистема технического (компьютерного) зрения;
- подсистема семантического анализа данных;
- подсистема хранения данных;
- подсистема отображения данных;
- подсистема поддержки принятия решений, выдачи управляющих сигналов, генерации вариантов реагирования на угрозы… – без этого нет интеллектуализации

Подсистема приёма и начальной обработки видеоинформации реализует функции:

- взаимодействия с источниками видеопотока (видеокамеры, видеорегистраторы и др.);
- получения видеопотока от источников видеопотока;
- организации промежуточного хранения видеоданных;
- подготовки видеоданных к дальнейшей обработке.

Подсистема приёма сигналов от охранных датчиков реализует функции взаимодействия с охранной системой и получения от неё информации о состоянии охранных датчиков. В настоящее время уже доступны интерфейсы для интегрирования таких датчиков как:

- Оптические (лазерные)
- Тепловые, инфракрасные
- Вибрационные
- Емкостные
- Сейсмические
- Магнитометрические
- Радиотехнические
- Радиолокационные
- Обрывные
- Доплеровские
- Датчики контроля функционального состояния сотрудников.

Подсистема компьютерного зрения использует технологии искусственного интеллекта и реализует функции:

- распознавания классов объектов (люди, транспортные средства, беспилотные летательные аппараты и т.д.);
- обнаружения людей и биообъектов;
- распознавания лиц людей (идентификация);
- распознавания государственных регистрационных номеров транспортных средств;
- распознавания характера действий объекта (стоит, движется, бежит, падает, выходит за пределы разрешенной траектории);
- ведения статистического учета времени пребывания посетителей, прогнозировать их потребности и подсказывать оптимальный поведенческий сценарий.

Использование технологий искусственного интеллекта позволяет подсистеме компьютерного зрения адаптироваться к изменяющимся внешним условиям.

Подсистема семантического анализа данных реализует функцию генерации текстового представления полученных данных.

Подсистема хранения реализует функции хранения в течение требуемого времени:

- исходных данных — видеоданных и сигналов, полученных от охранных датчиков;

- информации, полученной в ходе обработки данных подсистемой компьютерного зрения;
- информации, полученной в ходе обработки данных подсистемой семантического анализа данных.

Подсистема отображения данных реализует функции:

- поиска по массиву сохраненных данных;
- отображения данных за выбранное время в интерфейсе пользователя;
- комплексирования отображаемой информации перед отображением её в интерфейсе пользователя;
- интерпретация выходных данных в виде инфографики.

Подсистема поддержки принятия решений, выдачи управляющих сигналов, генерации вариантов реагирования на угрозы – обучаемая нейросеть, способная:

- накапливать сведения об успешных и негативных реализациях ситуационных сценариев;
- моделировать(генерировать) поведенческие траекториии должностных лиц;
- оптимизировать варианты в конкретных условиях;
- предлагать лицу, принимающему решения, оптимальные варианты действий по различным критериям – оперативность, обоснованность, стоимость, ущерб и т.д.

В качестве входных воздействий для программного продукта выступают:

- видеоданные, полученные от источников видеопотока;
- информация о состоянии охранных датчиков, полученная от охранной системы;
- действия, производимые пользователем в интерфейсе пользователя;
- ситуационная обстановка (суточные, климатические, природные и иные обстоятельства).

К выходным реакциям следует отнести:

- обработанные данные, сохраненные подсистемой хранения;
- информация, отображаемая в интерфейсе пользователя в результате действий пользователя, производимых в этом интерфейсе;
- варианты (подсказки) решений по реагированию на угрожающие ситуации;
- порядок автоматического оповещения правоохранительных, охранных и иных государственных служб об актах незаконного вмешательства и организация оперативного взаимодействия с ними.

Таким образом, кибербезопасность объекта может соответствовать перспективному набору угроз и достигается сочетанием мер организационного и технического характера [7, 34]. При этом в техническом плане используются различные аппаратные средства (генераторы помех, анализаторы спектра, анализаторы сигналов и т.п.), программы (файерволы, антивирусы, скремблеры и т.д.).

Литература

1. *Ведерников Ю.В., Гарькушев А.Ю., Сазыкин А.М.* Математическая формализация задачи оптимального построения информационно-управляющего комплекса мониторинга критически важных объектов //Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2014. – № 1-2 (67-68). – С. 26-31.

2. *Анисимов А.В.* Проблема сравнения и выбора варианта построения системы безопасности // Актуальные проблемы защиты и безопасности: Труды Четвертой Всероссийской научно-практической конференции.- Санкт-Петербург: Научно-производственное объединение специальных материалов 2001.- С. 348-351.

3. *Белов А.С., Скубьев А.В*. Эффективность обеспечения живучести подсистемы управления сложной организационно-технической системы // Телекоммуникации. 2020. № 11. С. 41-47.

4. *Анисимов В.Г., Анисимов Е.Г., Зегжда П.Д., Супрун А.Ф.* Проблема инновационного развития систем обеспечения информационной безопасности в сфере транспорта // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 27-32.

5. *Кащеев А.М., Кузин В.А., Лозицкий Р.М., Николаев Г.А., Ничипор В.И., Осипенко М.Н., Селиванов А.А., Шестихин А.В., Ямпольский С.М.* Межведомственное информационное взаимодействие в сфере обороны Российской Федерации: Военно-теоретический труд.- Москва: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, Военный институт (управления национальной обороной), 2017.- 198 с.

6. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. – 2019. – № 3. – С. 24-28.

7. *Anisimov V.G.* A risk-oriented approach to the control arrangement of security protection subsystems of information systems // Automatic Control and Computer Sciences, 2016, 50(8). С. 717-721. DOI: 10.3103/S0146411616080289

8. *Белов А.С., Трахинин Е.Л.* Моделирование возможных последствий внешних информационных воздействий на распределенную сеть связи // Телекоммуникации. 2020. № 12. С. 32-38.

9. *Зегжда П.Д.* Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем // Проблемы информационной безопасности. Компьютерные системы. 2018. № 1. С. 43-47.

10. *Анисимов Е.Г., Анисимов В.Г., Солохов И.В.* Проблемы научно-методического обеспечения межведомственного информационного взаимодействия // Военная мысль. 2017. № 12. С. 45-51.

11. *Гарькушев А.Ю., Селиванов А.А.* Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 7-8 (97-98). С. 12-16.

12. *Зегжда П.Д.* Эффективность функционирования компьютерной сети в условиях вредоносных информационных воздействий // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1 (45). С. 96-101.

13. *Ведерников Ю.В.* Формализация задачи выбора варианта структурного построения информационного комплекса управления многоуровневой иерархической системой по критерию информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 78-82.

14. *Бажин Д.А., Гарькушев А.Ю., Сазыкин А.М.* Модель оценки эффективности информационного обеспечения применения высокоточного оружия в контртеррористических операциях // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 1-2 (79-80). С. 44-53.

15. *Сауренко Т.Н., Присяжнюк С.П.* Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами // Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 140-145.

16. *Anisimov V.G., Anisimov E.G., Saurenko T.N., Zotova E.A.* Models of forecasting destructive influence risks for information processes in management systems // Information and Control Systems. 2019. № 5 (102). С. 18-23.

17. *Зегжда П.Д.* Методический подход к построению моделей прогнозирования показателей свойств систем информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2019. № 4. С. 45-49.

18. Anisimov V.G., Anisimov E.G., Saurenko T.N. Efficiency of ensuring the survivability of logistics information and control systems // B

сборнике: E3S Web of Conferences. Сер. "International Scientific and Practical Conference "Environmental Risks and Safety in Mechanical Engineering", ERSME 2020" 2020. С. 07025.

19. *Гарькушев А.Ю.* Модель информационного взаимодействия при обеспечении транспортной безопасности. // В сборнике: Актуальные проблемы защиты и безопасности. Труды XXIII Всероссийской научно-практической конференции Российской академии ракетных и артиллерийских наук (РАРАН), в 5 т.. Москва, 2020. С. 326-331.

20. *Богоева Е.М.* Формализация процедуры риск - ориентированного подхода при выполнении государственными органами контрольных функций // Вестник Российской таможенной академии. 2014. № 4. С. 96-102.

21. Зегжда П.Д. Модель формирования программы развития системы обеспечения информационной безопасности организации // Проблемы информационной безопасности. Компьютерные системы. 2021. № 2 (46). С. 109-117.

22. *Андреев В.П.* Информационная безопасность при чрезвычайных ситуациях: защита персональных компьютеров от несанкционированного доступа / *В.П. Андреев* [*и др.*] // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 11-12 (113-114). С. 109-114.

23. *Анисимов В.Г., Селиванов А.А., Анисимов Е.Г.* Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства // Информация и космос. 2016. № 4. С. 76-80.

24. *Зегжда П.Д.* Подход к оцениванию эффективности защиты информации в управляющих системах // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1 (41). С. 9-16.

25. *Гарькушев А.Ю.* Показатели качества перспективной системы управления на основе искусственного интеллекта для войск национальной гвардии. // В сборнике Комплексная безопасность и физическая защита. Труды VIII Мемориального семинара профессора Бориса Ефимовича Гельфанда и XV Международной научно-практической конференции. Санкт-Петербург, 2019. С. 189-196.

26. *Saurenko T.N.* Methodology control function realization within the electronic government concept framework // International Journal of Scientific and Technology Research. 2020. Т. 9. № 2. С. 6259-6262.

27. *Бажин Д.А., Барабанов В.В., Филиппов А.А.* Модели организации и проведения испытаний элементов системы информационного обеспечения применения высокоточных средств // Труды Военно-космической академии им. А.Ф. Можайского. 2015. № 648. С. 6-12.

28. *Сильников М.В.* Концептуальные основы информационно-аналитического обеспечения органов управления военной организацией государства // Известия Российской академии ракетных и артиллерийских наук. 2016. № 4 (94). С. 9-15.

29. *Ямпольский С.М.* Научно-методические основы информационно-аналитического обеспечения деятельности органов государственного и военного управления в ходе межведомственного информационного взаимодействия / *С.М. Ямпольский* [*и др.*].- Москва: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, Военный институт (управления национальной обороной). 2019.- 146 с.

30. *Анисимов Е.Г.,* Основы построения моделей интеллектуализации в системах безопасности / *Е.Г. Анисимов* [и др.] // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2014. № 9-10 (75-76). С. 22-27.

31 *Богоева Е.М., Липатова Н.Г.* Методика расчета латентного эффекта применения системы управления рисками // Вестник Российской таможенной академии. 2015. № 2. С. 115-123.

32. *Зегжда П.Д.* Модель оптимального комплексирования мероприятий обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2020. № 2. С. 9-15.

33. *Зегжда П.Д.* Модель и метод оптимизации вычислительных процессов в вычислительных системах с параллельной архитектурой / *П.Д. Зегжда* [*и др*.] // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4. С. 78-85.

34. *Анисимов Е.Г.* Метод распределения неоднородных ресурсов при управлении организационно-техническими системами // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 3-4 (93-94). С. 20-26.