Научная статья
УДК 004.056
doi: 10.24143/1812-9498-2021-2-35-42

Автоматизированная информационная система оценки и прогнозирования киберугроз на морских судах под флагом Российской Федерации: от субъектов киберугроз до этапов кибератаки

Алексей Валерьевич Когтев ✉

Государственный университет морского и речного флота им. адмирала С. О. Макарова, Санкт-Петербург, Россия, xx.ww.zz@ya.ru ✉

Аннотация. Рассматриваются и анализируются основные элементы разрабатываемой автоматизированной информационной системе оценки и прогнозирования киберугроз на морских судах под флагом Российской Федерации. Перечислены составляющие киберугроз: субъекты киберугроз, мотивы киберпреступников, задачи и цели киберпреступников, уязвимые судовые системы, предпосылки к реализации киберугроз, типы киберугроз и этапы кибератаки. Приведены примеры составляющих киберугроз. Обоснована вероятность внесения оперативных изменений в основные составляющие киберугроз, обусловленная развитием отраслей судоходства и прогрессом в сфере информационных технологий и киберугроз.

Ключевые слова: киберугрозы,킈бeринцидент, судно, киберпреступник, автоматизированная информационная система

Для цитирования: *Когтев А. В.* Автоматизированная информационная система оценки и прогнозирования киберугроз на морских судах под флагом Российской Федерации: от субъектов киберугроз до этапов кибератаки // Вестник Астраханского государственного технического университета. 2021. № 2 (72). С. 35–42. doi: 10.24143/1812-9498-2021-2-35-42.

Original article

Automated information system of assessing and predicting cyber threats on sea ships under Russian Federation flag: from subjects of cyber threats to stages of cyber-attack

Aleksey V. Kogtev ✉

Admiral Makarov State University of Maritime and Inland Shipping, Saint-Petersburg, Russia, xx.ww.zz@ya.ru ✉

Abstract. The article analyzes the main components of cyber threats in the developed automated information system for assessing and predicting cyber threats on sea vessels under the flag of the Russian Federation. The following components of cyber threats were listed: subjects of cyber threats, motives of cybercriminals, tasks and goals of cybercriminals, vulnerable ship systems, prerequisites for executing cyber threats, types of cyber threats, stages of a cyber-attack. The examples of the cyber-threat components are given. The possibility of making operational changes to the main components of cyber threats conditioned by the development of the shipping industries and progress of information technologies and cyber threats has been substantiated.

Keywords: cyber threats, cyber incident, vessel, cybercriminal, automated information system

For citation: Kogtev A. V. Automated information system of assessing and predicting cyber threats on sea ships under Russian Federation flag: from subjects of cyber threats to stages of cyber-attack. *Vestnik of Astrakhan State Technical University.* 2021;2 (72):35-42. (In Russ.) doi: 10.24143/1812-9498-2021-2-35-42.

Введение

В настоящее время общемировой тенденцией является цифровизация различных сфер экономики и ее отраслей. В полной мере это касается и отрасли морского транспорта: увеличивается количество автоматизированных процессов, активно развивается электронная навигация, происходят дистанционные обновления бортовых судовых систем во время плавания, датчики телеметрии передают на берег данные о состоянии систем судна и экипажа, у команды имеется возможность выхода в интернет и использования электронных ресурсов. Для того чтобы функционирование этих и многих других автоматизированных процессов не несло угроз безопасности судна и экипажа в рейсе и судоходной компании на берегу, необходимо выполнять требования по обеспечению кибербезопасности [1, 2].

Одним из решений, способных эффективно противодействовать киберугрозам и снижать вероятность наступления негативных последствий от их реализации, может стать автоматизированная информационая система оценки и прогнозирования киберугроз на морских судах под флагом Российской Федерации (далее – автоматизированная ИС) [1].

В настоящей статье рассмотрены основные составляющие киберугроз, которые будут анализироваться в автоматизированной ИС. Такими составляющими являются субъекты киберугроз, мотивы, задачи и цели киберпреступников, уязвимые судовые системы, предпосылки к реализации киберугроз, типы киберугроз и этапы кибератаки.

Субъекты киберугроз

Субъекты киберугроз обладают разной степенью навыков и ресурсов, чтобы потенциально угрожать безопасности судов и компаний.

Примеры основных субъектов киберугроз [3, 4]:

- случайные субъекты;
- собственные сотрудники;
- идеологически мотивированные личности (например, активисты, оппортунисты и др.);
- преступники и организованные преступные сообщества (в том числе хакерские);
- личности или компании-конкуренты;
- государства / государственные спонсируемые организации;
- террористы / террористические группировки.

Мотивы киберпреступников

В отличие от субъектов, которые непреднамеренно создали кибеинцидент, не имея на это мотива, большая часть субъектов имеет конкретную причину для организации и проведения кибератаки.

Основные мотивы для умышленной кибератаки на компании и суда могут быть разделены на следующие категории [4]:

- кибервандализм – преступная деятельность низкого уровня, включая нарушение работы систем, повреждение веб-сайтов и несанкционированный доступ к системам, данные действия могут быть совершены, например, начинающими хакерами;
- инсайдерская деятельность, совершаемая, например, недовольным персоналом или подрядчиками в целях мести;
- активизм – стремление к огласке, например средствами массовой информации, или оказание давления в интересах конкретной цели или причины;
- конкурентная деятельность – стремление создать конкурентное преимущество с целью нанести вред оппоненту, причинить финансовые или репутационные потери, например путем сбора бизнес-информации, кражи интеллектуальной собственности, сбора конкурентной информации о торгах или срыва бизнес-операций;
- шпионаж (в том числе промышленный и коммерческий шпионаж) – поиск несанкционированного доступа к конфиденциальной информации (интеллектуальная собственность, коммерческая информация, корпоративные стратегии, личные данные, образ жизни) и нарушение в государственных или коммерческих целях;
- организованная преступность – в основном движимая финансовой выгодой, может включать преступный ущерб, кражу груза, контрабанду товаров и людей, а также попытки уклониться от уплаты налогов и акцизов;
- терроризм – использование корабля для вселения страха и причинения физических и экономических потрясений;
- война – конфликт между национальными государствами, целью которого является нарушение перегрузочных систем, инфраструктуры, нарушения оперативного использования и вывод из строя судов или флота.

Задачи и цели киберпреступников

Мотивы злоумышленников определяют конкретные задачи и цели при кибератаке, которые они хотят достичь и которые будут определять влияние, оказываемое на систему и данные компании и судна.

Перечислим примеры задач и целей при кибератаке [3]:

− доступ к коммерчески чувствительным или конфиденциальным данным о грузе, команде, посетителях и пассажирах;
− манипулирование списками экипажа или пассажиров/посетителей, грузовыми манифестами, планами размещения или погрузочными листами;
− полный отказ в обслуживании в бизнес-системах, операционных и IT-системах судна;
− удаление критически важной информации о рейсе/грузе/пассажирах или другой служебной информации;
− мошенническая перевозка незаконных грузов или облегчение краж;
− нарушение нормальной работы компании, судовых систем и судов в целом;
− воспрепятствование обработке определенных грузов;
− требование выкупа за служебную или личную информацию;
− другие.

Уязвимые судовые системы

В свою очередь, задачи и цели киберпреступников могут быть реализованы с помощью использования различных уязвимых и слабых мест в судовых системах.

Уязвимые судовые системы могут включать [5]:

1. Мостовые системы:
− интегрированная система навигации;
− системы позиционирования (GPS и т. д.);
− информационная система отображения электронных карт (ECDIS);
− системы динамического позиционирования (DP);
− системы, которые взаимодействуют с электронными навигационными системами и системами движения/маневрирования;
− автоматическая идентификационная система (АИС);
− глобальная морская система связи при бедствии (ГМССБ);
− радиолокационное оборудование;
− регистраторы данных рейса (РДР);
− система аварийной сигнализации на мостике (BNWAS);
− судовые системы охранной сигнализации (SSAS).

Все более широкое использование цифровых сетевых навигационных систем с интерфейсом к прибрежным сетям для обновления и предоставления услуг делает такие системы уязвимыми для киберинцидентов. Мостовые системы, не подключенные к другим сетям, могут быть столь же уязвимы, поскольку съемные носители часто используются для обновления таких систем из других контролируемых или неконтролируемых сетей. Киберинцидент может распространяться на отказ в обслуживании или манипуляцию и, следовательно, может повлиять на все системы, связанные с навигацией, включая ECDIS, GNSS, AIS, VDR и Radar/ARPA.

2. Системы обработки грузов и управления:
− пункт управления грузами (CCR) и его оборудование;
− бортовые загрузочные компьютеры и компьютеры, используемые для обмена информацией о погрузке и обновлений плана погрузки с морским терминалом и стивидорной компанией;
− дистанционные системы отслеживания и обнаружения грузов и контейнеров;
− система индикации уровня;
− система дистанционного управления клапанами;
− системы водяного балласта;
− системы мониторинга рефрижераторов;
− система сигнализации попадания воды.

Цифровые системы, используемые для погрузки, управления и контроля грузов, включая опасные грузы, могут взаимодействовать с различными системами на берегу, включая порты, морские терминалы и стивидоры. Такие системы могут включать инструменты отслеживания отгрузки, доступные для грузоотправителей через сеть Интернет. Подобные интерфейсы делают системы управления грузами и данные в грузовых манифестах и списках погрузки уязвимыми для киберинцидентов.

3. Системы управления движением и механизмами, управления мощностью:
- регулятор двигателя;
- управление питанием;
- интегрированная система управления;
- сигнализация;
- система контроля трюмных вод;
- система очистки воды;
- мониторинг выбросов;
- мониторинг отопления, вентиляции и кондиционирования;
- системы контроля повреждений;
- другие системы мониторинга и сбора данных, например пожарная сигнализация.

Использование цифровых систем для мониторинга и управления бортовым оборудованием, движением и рулевым управлением делает такие системы уязвимыми для киберинцидентов. Уязвимость этих систем может возрасти при использовании в сочетании с дистанционным мониторингом на основе состояния и/или интеграции с навигационным и коммуникационным оборудованием на судах, использующих интегрированные мостовые системы.

4. Системы контроля доступа:
- системы наблюдения, такие как сеть видеонаблюдения;
- электронные системы бортового персонала.

Цифровые системы, используемые для поддержки контроля доступа для обеспечения физической безопасности и защиты судна и его груза, включая наблюдение, судовую охранную сигнализацию и электронные системы «персонал на борту», уязвимы для киберинцидентов.

5. Системы обслуживания пассажиров и управления ими:
- система управления недвижимостью (PMS);
- системы управления судном (часто включая электронные медицинские карты);
- системы, связанные с финансами;
- системы доступа пассажиров/посетителей/моряков на борт судна;
- системы поддержки инфраструктуры, такие как система доменных имен (DNS) и системы аутентификации/авторизации пользователей;
- системы управления инцидентами.

Цифровые системы, используемые для управления имуществом, посадки и контроля доступа, могут содержать ценные данные о пассажирах. Интеллектуальные устройства (планшеты, портативные сканеры и т. д.) сами по себе являются вектором атаки, поскольку в итоге собранные данные передаются в другие системы.

6. Сети общего пользования, обслуживания пассажиров и управления ими:
- пассажирский Wi-Fi и доступ в сеть Интернет по локальной сети (LAN) с возможностью подключать собственные устройства;
- гостевые развлекательные системы.

Фиксированные или беспроводные сети, подключенные к интернету, установленные на борту для удобства пассажиров, например гостевые развлекательные системы, должны считаться неконтролируемыми и не должны быть подключены к какой-либо критически важной для безопасности системе на борту.

7. Административные системы и системы социального обеспечения экипажа:
- административные системы;
- системы доступа к сети Wi-Fi или LAN для экипажа с возможностью подключения личных устройств.

Бортовые компьютерные сети, используемые для управления судном или обеспечения благополучия экипажа, особенно уязвимы при предоставлении доступа в сеть Интернет и электронной почты. Они могут быть использованы киберпреступниками для получения доступа к бортовым системам и данным. Эти системы следует рассматривать как неконтролируемые, их не следует подключать к какой-либо бортовой системе, критически важной для безопасности. Программное обеспечение, предоставленное управляющими компаниями или владельцами судов, также входит в данную категорию.

8. Системы связи:
− интегрированные системы связи;
− оборудование спутниковой связи;
− оборудование для передачи голоса через интернет (VOIP);
− беспроводные сети (WLAN);
− системы громкой связи и общей сигнализации;
− системы, используемые для сообщения обязательной информации государственным органам.

Доступность подключения к сети Интернет через спутник и/или другую беспроводную связь увеличивает уязвимость судов. Недавние исследования свидетельствуют, что, например, сигналы VSAT уязвимы для использования с недорогих мобильных устройств, способных принимать спутниковый сигнал. Следует учитывать системы связи с шифрованием и тщательно изучить механизмы киберзащиты, внедренные поставщиком услуг, но не следует полагаться исключительно на них для защиты каждой бортовой системы и данных. В эти системы включены каналы связи с государственными органами для передачи необходимой отчетной информации о судах и грузах. Применимые требования к управлению аутентификацией и контролем доступа со стороны этих органов должны строго соблюдаться. Также включены судовые возможности для сбора данных и опроса устройств и регистраторов данных, прикрепленных к грузам, для дальнейшей передачи назначенным получателям на берегу.

Помимо вышеуказанных категорий, можно выделить в отдельную категорию системы базовой инфраструктуры и системы защиты, включающие:
− шлюзы безопасности;
− маршрутизаторы;
− переключатели;
− межсетевые экраны;
− виртуальные частные сети (VPN);
− виртуальную сеть LAN (VLAN);
− системы предотвращения вторжений;
− системы регистрации событий безопасности.

Киберуязвимости как предпосылки к реализации киберугроз

Наличие уязвимых судовых систем не гарантирует киберпреступникам непосредственную реализацию киберугрозы и возникновение кибеинцидента. Но существуют уязвимости, являющиеся предпосылками для возможной реализации задуманного киберпреступниками. Данные уязвимости могут быть использованы, в том числе, через рассмотренные выше уязвимые судовые системы.

Ниже перечислены некоторые распространенные киберуязвимости, которые могут быть обнаружены на борту новых и существующих судов [3]:
− устаревшие и неподдерживаемые операционные системы;
− неактуальные (необновленные) версии системного программного обеспечения;
− устаревшее или отсутствующее антивирусное программное обеспечение и защита от вредоносных программ;
− неадекватные конфигурации безопасности, включая неэффективное управление сетью и использование учетных записей и паролей администраторов по умолчанию;
− судовые компьютерные сети, в которых отсутствуют меры защиты границ и сегментация сетей;
− критически важное для безопасности оборудование или системы, всегда подключенные к берегу;
− недостаточный контроль доступа к киберактивам, сетям и т. д. для третьих сторон, включая подрядчиков и поставщиков услуг;
− недостаточно обученный и/или квалифицированный персонал для управления киберрисками;
− отсутствующие, неадекватные или непроверенные планы и процедуры на случай непредвиденных обстоятельств.

Киберуязвимости на борту судов можно отнести к одной из следующих категорий:
− временные уязвимости, такие как дефекты программного обеспечения, устаревшие или неисправленные системы;

− ошибки технического проектирования, такие как управление доступом или неуправляемые сетевые соединения;

− ошибки реализации, например неправильно настроенные межсетевые экраны;

− процедурные или другие ошибки пользователя.

Отметим, что автономные системы будут менее уязвимы для внешних growинцидентов по сравнению с системами, подключенными к неконтролируемым сетям или напрямую подключенными к сети Интернет. Следует понимать, какие важные судовые системы и каким образом подключены к неконтролируемым сетям, и учитывать человеческий фактор, т. к. многие инциденты инициируются действиями персонала.

Типы киберугроз

Существуют две категории киберугроз, которые могут затронуть компании и суда [3]:

− нецелевые атаки, когда системы и данные компании или судна являются одной из многих потенциальных целей;

− целевые атаки, когда системы и данные компании или судна являются предполагаемой целью или одной из нескольких целей.

Нецелевые атаки могут использовать инструменты и методы, доступные в сети Интернет, для обнаружения и использования широко распространенных уязвимостей, которые могут существовать в компании и на борту судна. Примеры некоторых инструментов и методов, которые могут использоваться в этих обстоятельствах, включают:

− вредоносное программное обеспечение, предназначенное для доступа к компьютеру или его повреждения, модификации и несанкционированного доступа к файлам без ведома владельца. Существуют различные типы вредоносных программ, включая трояны, программы-вымогатели, шпионское программное обеспечение, вирусы и черви;

− эксплойты. Термин «эксплойт» обозначает компьютерную программу, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на систему [6]. Этими уязвимостями могут быть, например, ошибка кода, неисправность оборудования и/или ошибка в реализации протокола. Данные уязвимости могут использоваться удаленно или запускаться локально, например часть вредоносного кода может выполняться пользователем через ссылки, распространяемые во вложениях электронной почты или через вредоносные веб-сайты;

− «водопой» – создание поддельного веб-сайта или взлом подлинного веб-сайта для использования ничего не подозревающих посетителей;

− сканирование – произвольный поиск в больших частях интернета уязвимостей, которые можно использовать;

− тайпсквоттинг, или перехват URL-адресов, поддельный URL-адрес. Основывается на ошибках, таких как опечатки, сделанные интернет-пользователями при вводе адреса веб-сайта в веб-браузер. Если пользователь случайно введет неправильный адрес веб-сайта, он может попасть на альтернативный и зачастую вредоносный веб-сайт.

Целевые атаки могут быть более изощренными и использовать инструменты и методы, специально созданные для нацеливания на определенную компанию или судно. Примеры инструментов и методов, которые могут использоваться в этих обстоятельствах, включают:

− социальную инженерию – нетехнический метод, используемый для манипулирования инсайдерами с целью нарушения процедур безопасности и получения информации, обычно посредством взаимодействия через социальные сети и электронную почту;

− брутфорс – атака с перебором множества паролей в надежде угадать их правильно. Злоумышленник систематически проверяет все возможные пароли, пока не будет найден правильный;

− credential stuffing – использование ранее скомпрометированных учетных данных или определенных часто используемых паролей для попытки несанкционированного доступа к системе или приложению;

− отказ в обслуживании (DoS, DDoS), который не позволяет законным и авторизованным пользователям получить доступ к информации, обычно путем наводнения сети данными. Распределенная атака типа «отказ в обслуживании» (DDoS) берет под контроль несколько компьютеров и/или серверов для реализации DoS-атаки;

− фишинг – отправка электронных писем большому количеству потенциальных целей с просьбой предоставить определенные фрагменты конфиденциальной информации. Электронное письмо также может содержать вредоносное вложение или запрос на посещение человеком поддельного веб-сайта с использованием гиперссылки, содержащейся в электронном письме;

− целевой фишинг, когда жертвами становятся личные электронные письма, часто содержащие вредоносное программное обеспечение или ссылки, которые автоматически загружают вредоносное программное обеспечение;

− подрыв цепочки поставок – кибератака на компанию или судно путем компрометации оборудования, программного обеспечения или вспомогательных услуг, предоставляемых компании или судну.

Приведенные выше примеры не являются исчерпывающими, развиваются и другие методы кибератак. С учетом прогресса в области автономного судоходства следует ожидать появления новых киберугроз, нацеленных на данное направление. Возможное количество и изощренность инструментов и методов, используемых в кибератаках, продолжают развиваться и ограничиваются только изобретательностью тех организаций и отдельных лиц, которые их разрабатывают.

Этапы кибератаки

Продолжительность времени на подготовку кибератаки может определяться мотивами и целями злоумышленника, а также устойчивостью технических и процедурных средств защиты, реализуемых компанией, в том числе на судне и в компании.

При рассмотрении целевых кибератак обычно наблюдаются следующие стадии:

1. Обследование/разведка. Открытые и общедоступные источники, такие как социальные сети, используются для получения информации о потенциальной цели (например, компании, судне или члене экипажа) при подготовке к кибератаке. Социальные сети, технические форумы и скрытые свойства веб-сайтов, документов и публикаций могут использоваться для выявления технических, процедурных и физических уязвимостей. Использование открытых/общедоступных источников может быть дополнено мониторингом (сниффингом) фактических данных, поступающих в/из компании или судна;

2. Доставка. Киберпреступники могут попытаться получить доступ к системам и данным компании и судна. Это может быть сделано либо внутри компании, либо на судне, либо удаленно через подключение к сети Интернет.

Примеры методов, используемых для получения доступа:

− онлайн-сервисы компании, включая системы отслеживания грузов или контейнеров;

− отправка сотрудникам электронных писем, содержащих вредоносные файлы или ссылки на вредоносные веб-сайты;

− предоставление зараженных съемных носителей, например как часть обновления программного обеспечения бортовой системы;

− создание ложных или вводящих в заблуждение веб-сайтов, которые поощряют раскрытие персоналом информации об учетной записи пользователя;

3. Нарушение. Степень, в которой киберпреступник может взломать систему компании или судна, будет зависеть от значимости обнаруженной уязвимости и выбранного метода атаки. Следует отметить, что нарушение может не привести к каким-либо очевидным изменениям в состоянии оборудования. В зависимости от серьезности нарушения киберпреступник может:

− вносить изменения, влияющие на работу системы, например прерывать или изменять информацию, используемую навигационным оборудованием;

− получать доступ, делать копии или изменять оперативно важную информацию, такую как списки погрузки, или коммерчески конфиденциальные данные, такие как грузовые манифесты и/или списки членов экипажа и пассажиров/посетителей;

− достичь полного контроля над системой, например системой управления оборудованием;

4. Поворот. Это метод использования уже скомпрометированной системы для атаки на другие системы в той же сети. На этом этапе атаки киберпреступник использует первую скомпрометированную систему для атаки на другие недоступные системы. Как правило, атаке подвергается наиболее уязвимая часть системы жертвы с самым низким уровнем безопасности. После получения доступа киберпреступник попытается взломать остальную систему.

Обычно на этапе поворота киберпреступник может попытаться:

− загружать в систему инструменты, эксплойты и скрипты для облегчения нового этапа атаки;

− выполнять обнаружение соседних систем с помощью инструментов сканирования или отображения сети;

− установить постоянные инструменты или регистратор ключей для сохранения и поддержания доступа к системе;
− выполнять новые атаки на систему.

Заключение

В статье были рассмотрены основные составляющие киберугроз, информация и данные по которым будут анализироваться в автоматизированной ИС для каждого конкретного киберинцидента. Для этого в автоматизированной ИС предусмотрены соответствующие модули, подсистемы и базы данных.

Отметим, что развитие отраслей судоходства, информационных технологий и киберугроз может потребовать внесения оперативных изменений в рассмотренные нами основные составляющие киберугроз, особенно в части, касающейся уязвимых судовых систем и типов киберугроз.

СПИСОК ИСТОЧНИКОВ

1. *Когтев А. В.* Проблемы создания единой отраслевой политики по кибербезопасности в сфере морского транспорта // Региональная информатика и информационная безопасность: сб. тр. СПб.: Изд-во СПОИСУ, 2020. Вып. 9. С. 95–96.
2. *Судоходство* в аспекте кибербезопасности // Мор. вести. 2019. № 18. URL: http://www.morvesti.ru/analitika/1689/82714/ (дата обращения: 10.10.2021).
3. *The Guidelines* on cyber security onboard ships. Version 4. BIMCO, 2020. 61 p.
4. *Code* of Practice. Cyber Security for Ships. Institution of Engineering and Technology, London, United Kingdom, 2017. 73 p.
5. *MSC-FAL*.1/Circ.3 on Guidelines on maritime cyber risk management. International Maritime Organization, London, 2017. 4 p.
6. *Эксплойт.* URL: https://ru.wikipedia.org/wiki/Эксплойт/ (дата обращения: 10.10.2021).

REFERENCES

1. Kogtev A. V. Problemy sozdaniia edinoi otraslevoi politiki po kiberbezopasnosti v sfere morskogo transporta [Problems of creating unified sectoral cybersecurity policy in maritime transport system]. *Region-al'naia informatika i informatsionnaia bezopasnost': sbornik trudov.* Saint-Petersburg, Izd-vo SPOISU, 2020. Iss. 9. Pp. 95-96.
2. Sudokhodstvo v aspekte kiberbezopasnosti [Shipping in terms of cybersecurity]. *Morskie vesti,* 2019, no. 18. Available at: http://www.morvesti.ru/analitika/1689/82714/ (accessed: 10.10.2021).
3. *The Guidelines on cyber security onboard ships*. Version 4. BIMCO, 2020. 61 p.
4. *Code of Practice. Cyber Security for Ships.* Institution of Engineering and Technology, London, United Kingdom, 2017. 73 p.
5. *MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management.* International Maritime Organization, London, 2017. 4 p.
6. *Eksploit* [Exploit]. Available at: https://ru.wikipedia.org/wiki/Eksploit/ (accessed: 10.10.2021).

Статья поступила в редакцию 18.10.2021; одобрена после рецензирования 29.10.2021; принята к публикации 03.11.2021.
The article was submitted 18.10.2021; approved after reviewing 29.10.2021; accepted for publication 03.11.2021.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Алексей Валерьевич Когтев − аспирант кафедры комплексного обеспечения информационной безопасности; Государственный университет морского и речного флота им. адмирала С. О. Макарова; 198515, Санкт-Петербург, ул. Двинская, 5/7; xx.ww.zz@ya.ru

INFORMATION ABOUT THE AUTHOR

Aleksey V. Kogtev – Postgraduate Student of the Department of Integrated Assurance of Information Security; Admiral Makarov State University of Maritime and Inland Shipping; 198035, Saint-Petersburg, Dvinskaya St., 5/7; xx.ww.zz@ya.ru