УДК: 004.056 DOI: 10.53816/23061456_2022_1–2_64

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

A MODEL OF INFORMATION SECURITY THREATS OF PROTECTED SPECIAL-PURPOSE INFORMATION AND ANALYTICAL SYSTEMS

Канд. техн. наук С.А. Диченко

Ph.D. S.A. Dichenko

Краснодарское высшее военное училище им. С.М. Штеменко

Экспоненциальный рост объема и ценности информации, обрабатываемой в автоматизированных системах различного назначения, в том числе военного, большое количество источников и потребителей информации, их организационная и территориальная распределенность способствовали созданию и использованию в интересах силовых ведомств Российской Федерации Центров обработки данных и, как следствие, широкому развитию и внедрению технологий работы с большими данными (Big Data). Появление в Вооруженных Силах Российской Федерации новых направлений развития, связанных с обработкой и хранением больших данных, осложняющееся возникновением новых угроз безопасности информации, требует совершенствования существующих и разработки новых методов защиты информации, адекватность и результативность которых напрямую зависит от качества используемой модели угроз безопасности информации.
Ключевые слова: Big Data, центр обработки данных, информационно-аналитические системы специального назначения, модель угроз безопасности информации, деструктивные воздействия злоумышленника, нарушение целостности данных.

The exponential growth in the volume and value of information processed in automated systems for various purposes, including military, a large number of sources and consumers of information, their organizational and territorial distribution, contributed to the creation and use of Data Processing Centers in the interests of law enforcement agencies of the Russian Federation and, as a result, the widespread development and introduction of technologies for working with big data (Big Data). The emergence of new directions of development in the Armed Forces of the Russian Federation related to the processing and storage of Big Data, complicated by the emergence of new threats to information security, requires the improvement of existing and the development of new methods of information protection, the adequacy and effectiveness of which directly depends on the quality of the information security threat model used.
Keywords: Big Data, data processing center, information and analytical systems for special purposes, information security threat model, destructive effects of an attacker, violation of data integrity.

Введение

Активное внедрение перспективных информационных технологий при создании автоматизированных систем специального назначения (АС СН), получивших в настоящее время широкое применение в войсках, непрерывное изменение состава и содержания решаемых задач характеризуется повышением рисков нарушения работоспособности таких систем в условиях деструктивных воздействий [1–4]. Результатом разрушающих воздействий злоумышленника на АС СН является снижение их устойчивости и, как следствие, снижение эффективности системы вооружения Вооруженных Сил Российской Федерации (ВС РФ) в целом.

Вопросу построения устойчивых АС СН посвящено достаточно много научных и практических работ [1–5], в которых задача решается через обеспечение их живучести, надежности и помехоустойчивости. Однако сохранять во времени в установленных пределах значения всех параметров, характеризующих способность системы выполнять свои функции в заданных режимах и условиях эксплуатации (надежность), а также в условиях воздействий внешней среды и отказов компонентов системы в заданных пределах (живучесть), в том числе в условиях воздействия помех, в частности, от электромагнитных полей (помехоустойчивость) для повышения устойчивости АС СН, результатом функционирования которых является представление выходной информации для последующего использования, является недостаточным.

В виду того, что основной целью функционирования информационных систем является удовлетворение потребностей в обеспечении надежного и своевременного представления полной, достоверной и конфиденциальной информации, важным для таких систем является обеспечение безопасности обрабатываемой в них информации. При этом особую актуальность обеспечение безопасности информации (БИ), в частности, обеспечение ее целостности, приобретает для устойчивого функционирования информационно-аналитических систем специального назначения (ИАС СН) в условиях деструктивных воздействий злоумышленника [6–8].

Необходимость обеспечения целостности информации в ИАС СН обуславливается строгостью предъявляемых к ним требований по обеспечению своевременности и правильности принимаемого пользователем системы решения, выполнение которых напрямую зависит от обеспечения полноты и достоверности обрабатываемой в них информации. Для определения возможных объектов воздействий, источников, способов реализации (возникновения) актуальных угроз БИ, характеризуемых нарушением целостности информации, обрабатываемой в ИАС СН, требуется выполнить оценивание угроз БИ и построить модель угроз БИ ИАС СН.

На основе результатов, полученных в работе [9], разработан обобщенный алгоритм построения модели угроз БИ ИАС СН (рис. 1), для определения границ и обеспечения полноты которой необходимо проанализировать условия и среду функционирования ИАС СН.

Исследование условий и среды функционирования ИАС СН

Задачами любой ИАС СН являются эффективное хранение, обработка и анализ данных, полученных из целого ряда источников, в том числе внешних.

Внешним оперативным источником данных (ОИД) для ИАС СН являются используемые в современных условиях постоянного роста объема и ценности обрабатываемой в АС СН информации Центры обработки данных (ЦОД) ВС РФ.

Архитектура современной ИАС СН в обобщенном виде представлена на рис. 2.

Внедряемые в ВС РФ территориально-распределенные ЦОД являются материальной основой построения банков данных для функционирования существующих и разрабатываемых АС СН (рис. 3).

При этом угрозы БИ ИАС СН должны оцениваться в общем как для самой ИАС СН, так и для информационно-телекоммуникационной инфраструктуры ЦОД ВС РФ, на базе которой они функционируют.

Описание объекта защиты и возможных негативных последствий от реализации (возникновения) угроз БИ

Результатом функционирования ИАС СН является обеспечение своевременности и правиль-

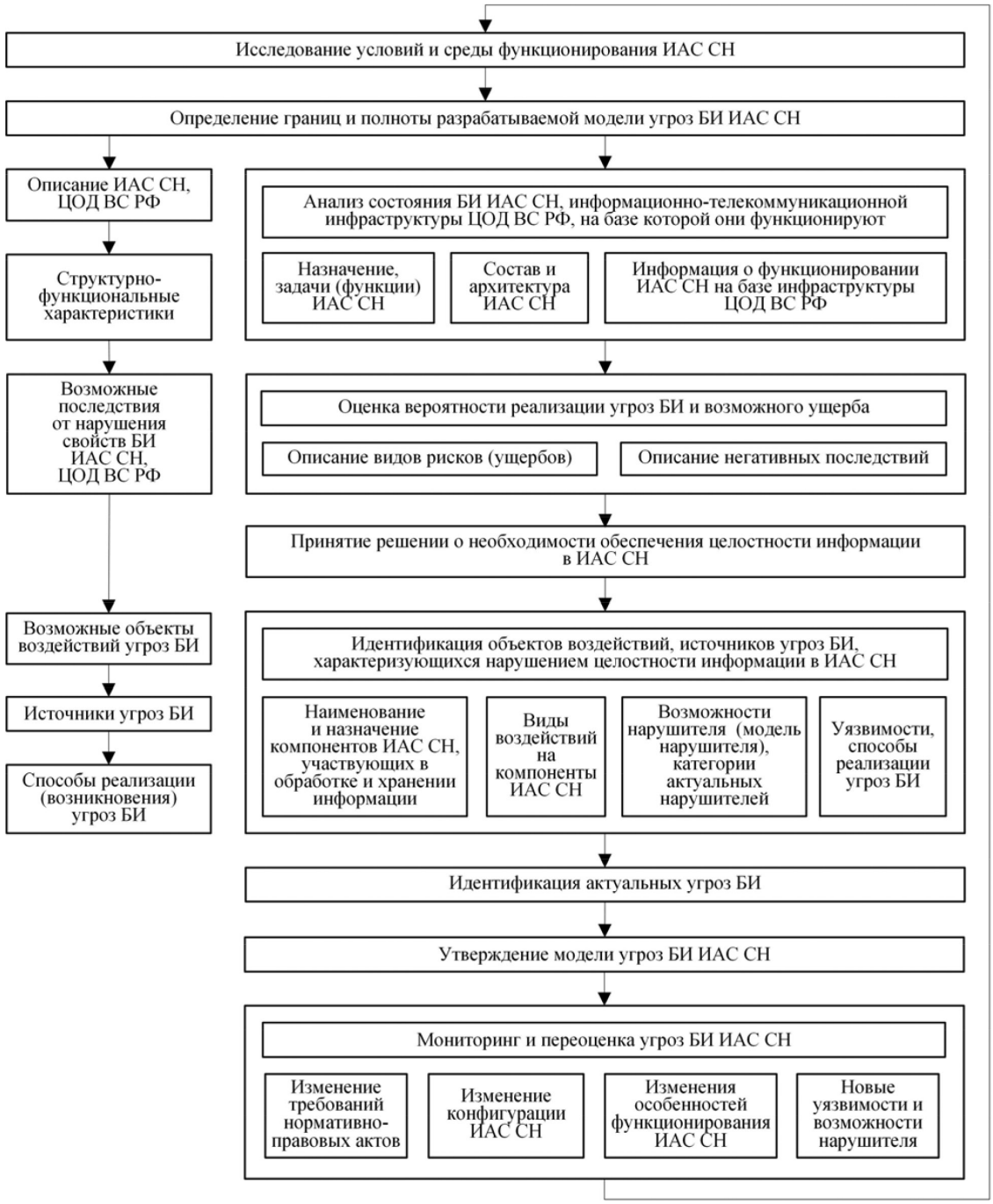

Рис. 1. Обобщенный алгоритм построения модели угроз БИ ИАС СН

ности принимаемого пользователем системы решения. Поэтому одним из наиболее негативных последствий от реализации (возникновения) угроз БИ ИАС СН является снижение вероятности выполнения задачи целевого функционирования ИАС СН или вообще ее невыполнение.

Невозможность своевременного принятия пользователем ИАС СН правильного решения напрямую зависит от полноты и достоверности хранящейся, обрабатываемой и анализируемой в них информации, то есть от обеспечения ее целостности.

Важнейшей и наиболее уязвимой по отношению к деструктивным воздействиям, приводящим к нарушению целостности информации, подсистемой ИАС СН, а также ЦОД ВС РФ явля-

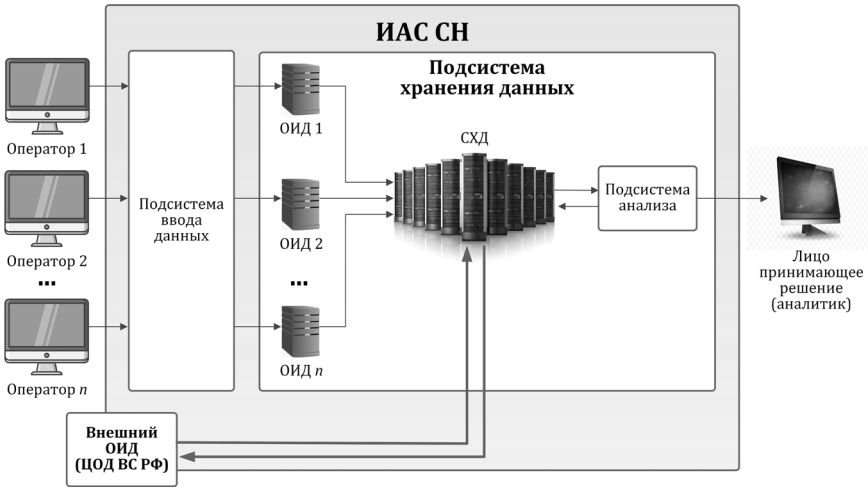

Рис. 2. Обобщенная структура ИАС СН

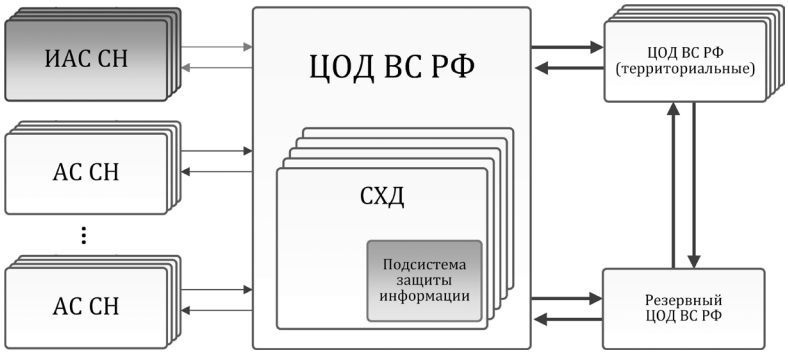

Рис. 3. Схема взаимодействия ЦОД ВС РФ и ИАС СН

ется система хранения данных (СХД), имеющая различные архитектуры построения.

Задача хранения данных при незначительном увеличении их объемов традиционно решается путем наращивания ёмкости хранилищ данных с архитектурой DAS (Direct-Attached Storage). Поэтому СХД на основе архитектуры DAS представляет собой совокупность устройств внешней памяти, подключенных напрямую к серверу и используемых только сервером. В настоящее время использование в интересах ИАС СН множества СХД с архитектурой DAS является нецелесообразно, это приводит к появлению распределенных по всей сети локальных СХД. Это усложняет расширение хранилища данных, так как эти системы не поддерживают совместного использования ёмкости хранения разными серверами и разделения данных между ними.

В отличии от архитектуры DAS сетевое хранение данных, предусматривающее централизованное хранение данных, гибкость при использовании информации, повышение надежности и безопасности хранения данных в СХД, реализована в рамках двух технологий: сетевых хранилищ NAS (Network Attached Storage), сетей хранения SAN (Storage Area Network).

В свою очередь, NAS — система, позволяющая централизованно хранить данные и удалённо получать доступ к этим данным всем авторизованным пользователям. Такой отдельный файл-сервер позволяет разделить хранилище данных на отдельные части. Пользователи сети, распределённые по группам, получают доступ только к определенной части массива данных, доступ к остальной информации им запрещен [12, 13]. К тому же в СХД на основе NAS отсутствует возможность использования хранилища устройства, подключаемого по локальной сети. В виду того, что доступ к данным осуществляется не на уровне блоков, а на уровне целых файлов, а также средой передачи для NAS-сервера служит сеть Ethernet, производительность работы такого хранилища не в полной мере соответствует требованиям, предъявляемым к СХД,

применяемым в интересах ИАС СН. Поэтому, учитывая недостатки такой системы, технология NAS нечасто используются в СХД, применяемых в интересах ИАС СН.

При этом сеть хранения SAN является отделённой от локальной сети и может хранить огромные объёмы информации с возможностью практически бесконечного наращивания. Обычно SAN — это множество подключенных к коммутатору массивов, составленных из хранилищ данных. Коммутатор соединяется с серверами, которые ответственны за организацию доступа к хранимым данным. SAN осуществляет доступ любого сервера к любому накопителю без дополнительных нагрузок на локальную сеть. Для обмена данными не обязательно участие серверов. Сеть хранения SAN отличается высокой эффективностью и безотказностью работы. Последние тенденции в SAN сводятся к использованию виртуализации памяти. Это даёт серверам возможность, к примеру, создать один логический том из нескольких устройств хранения. Безопасность обеспечивается на уровне сервера, в то время как в NAS — на уровне доступа к файлам. Однако наличие у злоумышленника возможности несанкционированного доступа (НСД) к одному или нескольким узлам, которые расположены в единой сети, может нанести ощутимый ущерб системе.

Для обеспечения целостности информации при разработке СХД внимание, главным образом, уделяется повышению надежности средств хранения при сбоях и отказах, вызванных, в первую очередь, деструктивными воздействиями среды. Поэтому широкое развитие получили системы резервирования и архивирования информации на дополнительные носители, построение каналов для тиражирования данных на альтернативные площадки и т.д. При этом задача обеспечения целостности информации в условиях деструктивных воздействий злоумышленника традиционно решается посредством построения защищенных информационных систем хранения и обработки данных с реализованным комплексом средств защиты информации. Обобщенная модель защищенной информационной системы хранения и обработки данных в условиях применения злоумышленником специальных организационно-технических мер программно-технических средств (информационного оружия) представлена в работе. Однако данная модель в большей степени отражает меры защиты информации в процессе ее обработки и не учитывает вероятные воздействия злоумышленника на процесс хранения данных в современных СХД, применяемые в интересах ИАС СН, в том числе в ЦОД ВС РФ.

Результаты проведенного анализа позволяют сделать вывод о том, что в разрабатываемой модели угроз БИ ИАС СН объект защиты должен включать в себя не только СХД ИАС СН, но и СХД ЦОД ВС РФ, которая в современных условиях развития ВС РФ является важнейшим внешним ОИД (рис. 4).

Источники угроз БИ ИАС СН (модель нарушителя)

Источники угроз БИ ИАС СН могут быть как внешние, так и внутренние. При этом угроза БИ ИАС СН часто является следствием наличия уязвимостей в конкретных узлах сети хранения. Возможные уязвимости определяют составляющие элементы и свойства архитектурных решений сетей хранения, а именно: элементы архитектуры, протоколы обмена, интерфейсы, аппаратные платформы, системное программное обеспечение, условия эксплуатации, территориальное размещение узлов сети хранения. Поэтому возможности нарушителя по эффективному воздействию на процессы функционирования ИАС СН часто рассматриваются в зависимости от их архитектуры и архитектуры построения СХД.

СХД, основанные на технологиях NAS и SAN, применяемые в интересах ИАС СН, из-за особенностей архитектуры обладают недостаточной защитой. При этом существующие уязвимости необходимо рассматривать на всех уровнях предоставления служб, которые напрямую влияют на БИ.

При рассмотрении SAN-системы на уровне устройств можно прийти к выводу, что угроза НСД возникает в основном из-за недостаточной сложности пароля и ненадёжной системы авторизации пользователей. В таком случае НСД с привилегированного пользователя даёт полный контроль над данным узлом, из-за чего возникает угроза безопасности хранимых данных.

Также существует уязвимость встроенного программного обеспечения. Пониженное внима-

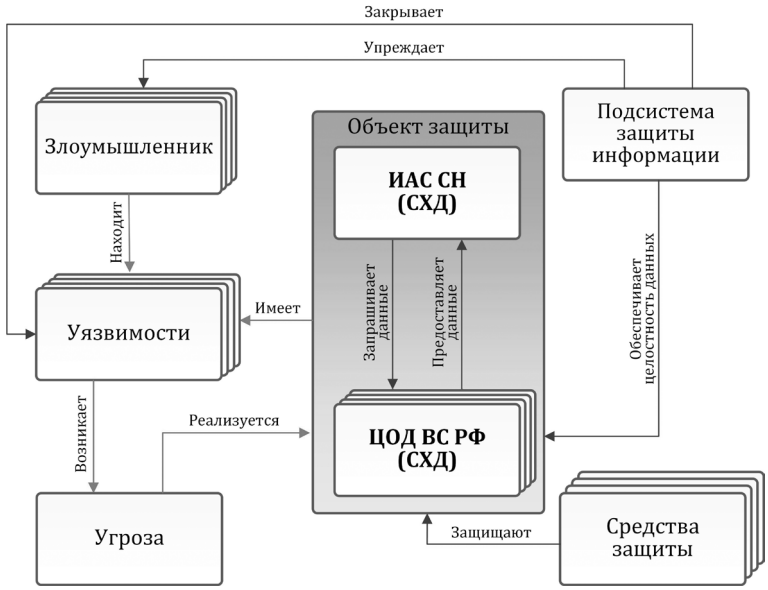

Рис. 4. Пояснение порядка взаимодействия подсистемы защиты информации и злоумышленника

ние к безопасности кода зачастую приводит к использованию нарушителем уязвимых устройств и проведение им удалённых атак на остальные устройства сети.

В свою очередь, NAS-системы на уровне устройств работают по принципу «файл-сервер». Однако обычно получить доступ к хранилищу невозможно без элементов SAN. Традиционно это хранилища в виде жестких дисков, которые подключаются к серверу с помощью оптических линий. В этом случае к безопасности NAS должны быть предъявлены такие же требования, как и к безопасности SAN-решений.

На уровне данных при НСД с правами администратора нарушитель имеет возможность полностью контролировать данные, из-за чего возникает опасность блокирования доступа, искажения или удаления информации. В виду того, что архитектура SAN работает таким образом, что сервера и рабочие станции подключаются с единой зоной доступа к устройствам хранения, безопасность доступа к данным должна обеспечиваться не только на стороне сервера, но и на стороне пользователей.

На уровне сетевого взаимодействия частой угрозой является несанкционированное подключение к каналам с подменой адресов. В виду того, что SAN является открытой архитектурой, а осуществляющее коммутацию и конвертацию оборудование работает удалённо — это может привести к модификации данных нарушителем. В свою очередь, для NAS из-за того, что их сетевой уровень в большинстве случаев работает по протоколу TCP/IP, основную угрозу представляют сетевые атаки.

Все используемые средства управления доступом к данным должны выполнять самые строгие требования безопасности. Это относится не только к конкретным устройствам, но и к архитектуре в целом. Должен выполняться контроль за пользователями с правами доступа и осуществляться централизованный контроль за работой устройств.

Возможные угрозы БИ и наличие уязвимостей должно учитываться при построении модели нарушителя. При этом подходы Федеральной службы безопасности России (ФСБ) и Федеральной службы по техническому и экспертному контролю России (ФСТЭК) к формированию модели нарушителя несколько отличаются. ФСБ отвечает за регулирование в области криптографии и ее методика в основном служит для выбора класса криптосредств. Соответственно, ФСБ при описании нарушителя делает упор на возможностях нарушителя по атакам на криптосредства. В свою очередь, методика ФСТЭК более широкая и описывает возможности нарушителя по атакам на систему в целом.

Результаты анализа условий и среды функционирования ИАС СН, возможных негативных последствий от реализации (возникновения) угроз БИ, а также возможностей нарушителя по эффективному воздействию на процессы функционирования объекта защиты позволяют сделать вывод

о том, что категориями актуальных нарушителей являются внутреннии нарушители, описание характеристик которых выполнено на основе обобщения двух подходов ФСБ и ФСТЭК:

– пользователи системы с возможностью самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы криптосредства;

– администраторы системы и администраторы безопасности с возможностью привлекать специалистов, имеющих опыт разработки и анализа средств криптографической защиты информации.

Способы реализации (возникновения) угроз БИ ИАС СН

Степень реализации цели функционирования ИАС СН зависит от совокупности объективных и субъективных факторов, воздействующих на обрабатываемую в них информацию. При этом целостность информации в СХД обычно нарушается в результате как случайных ошибок, так и преднамеренного несанкционированного изменения данных (например, посредством действия вредоносного кода) или выхода из строя части носителя (например, отдельных ячеек, секторов).

На машинном языке представления данных, под нарушением их целостности понимается следующее: инверсия битов; добавление новых битов; стирание битов; изменение порядка следования битов.

Актуальные угрозы БИ ИАС СН

Угрозы БИ принято классифицировать по различным признакам, одним из которых является «результат реализации». Угрозы БИ по данному классификационному признаку подразделяются на: угрозы, приводящие к нарушению конфиденциальности, целостности и доступности.

Классификация угроз БИ «по результату», приводящие к нарушению ее целостности в СХД, представлена на рис. 5.

После определения категорий актуальных нарушителей БИ и соответствующих им угроз, содержащихся в банке данных угроз БИ ФСТЭК, актуальными угрозами БИ ИАС СН, характеризующиеся нарушением целостности информации, являются:

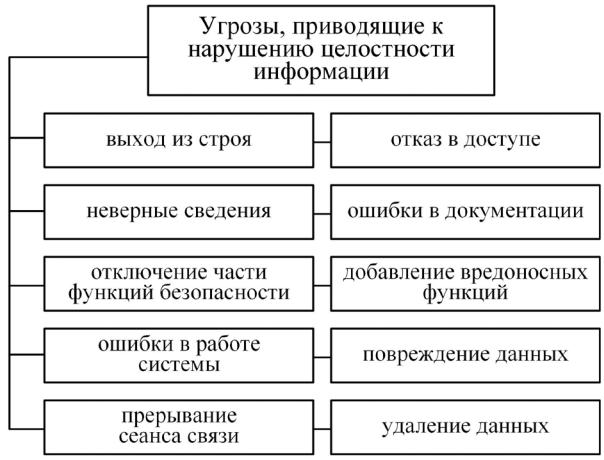

Рис. 5. Классификация угроз БИ, приводящих к нарушению ее целостности

– угроза повышения привилегий (УБИ. 122);

– угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 143);

– угроза наличия механизмов разработчика (УБИ. 169);

– угроза несанкционированного воздействия на средство защиты информации (УБИ. 187);

– угроза перехвата управления информационной системой (УБИ. 212);

– угроза использования скомпрометированного доверенного источника обновлений программного обеспечения (УБИ. 217) и т.д.

Вывод

Представлена оценка угроз БИ и построена модель угроз БИ (нарушителя) ИАС СН. Определены возможные объекты воздействий, источники, способы реализации (возникновения) актуальных угроз БИ, характеризуемые нарушением целостности информации, обрабатываемой в ИАС СН.

Результаты, полученные при анализе уязвимостей в СХД, а также возможностей злоумышленника по эффективному воздействию на процессы функционирования ИАС СН, позволяют определить направления в области совершенствования существующих и разработки новых методов защиты информации от угроз нарушения целостности, реализуемых посредством деструктивных воздействий злоумышленника на СХД ИАС СН.

Литература

1. Гончаренко В.А. Концептуальные основы построения устойчивых к воздействиям автоматизированных систем специального назначения на основе адаптивных технологий // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 4. С. 38–47.

2. Есиков Д.О. Задачи обеспечения устойчивости функционирования распределенных информационных систем // Программные продукты и системы. 2015. № 4 (112). С. 133–141.

3. Легков К.Е., Буренин А.Н. Об устойчивости управления серверным оборудованием современных инфокоммуникационных сетей специального назначения // T-comm: Телекоммуникации и транспорт. 2014. Т. 8. № 12. С. 47–50.

4. Петренко С.А. Проблема устойчивости функционирования киберсистем в условиях деструктивных воздействий // Труды института системного анализа Российской академии наук. 2010. Т. 52. С. 68–105.

5. Хомоненко А.Д., Басыров А.Г., Бубнов В.П. и др. Модели и методы исследования информационных систем. — СПб: Лань. 2019. 204 с.

6. Диченко С.А., Финько О.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Вопросы кибербезопасности. 2019. № 6 (34). С. 17–36.

7. Диченко С.А., Финько О.А. Снижение вводимой избыточности при обеспечении устойчивости информационно-аналитических систем в условиях компенсации последствий деструктивных воздействий злоумышленника // Автоматизация процессов управления. 2020. № 4 (62). С. 38–48.

8. Диченко С.А., Финько О.А. Контроль и восстановление целостности данных в защищенных информационно-аналитических системах // Труды Военно-космической академии им. А.Ф. Можайского. 2021. № 676. С. 36–49.

9. Викторов Е.А., Иванин А.Н., Канаев А.К. Методика обеспечения устойчивости функционирования транспортной сети связи специального назначения в условиях реализации сетевых и компьютерных атак // Труды Военно-космической академии им. А.Ф. Можайского. 2020. № 672. С. 92–101.

References

1. Goncharenko V.A. Conceptual bases for building resilient to the impacts of automated systems for special purposes based on adaptive technologies. H&ES Research. 2018. Vol. 10. № 4. P. 38–47.

2. Yesikov D.O. Tasks of ensuring the stability of the functioning of distributed information systems. Software products and systems. 2015. № 4 (112). P. 133–141.

3. Legkov K.E., Burenin A.N. About stability of control of the server equipment of the modern infocommunication networks of the special purpose // T-comm: Telecommunications and transpor. 2014. Vol. 8. № 12. P. 47–50.

4. Petrenko S.A. The problem of the stability of the functioning of cybersystems in the conditions of destructive influences. Proceedings of the Institute of System Analysis of the Russian Academy of Sciences. 2010. Vol. 52. P. 68–105.

5. Khomonenko A.D., Basyrov A.G., Bubnov V.P. Models and methods of research of information systems. — St. Petersburg: Lan Publishing House. 2019. 204 p.

6. Dichenko S.A., Finko O.A. Hybrid crypto-code method for monitoring and recovery of data integrity for protected information and analytical systems. Cybersecurity Issues. 2019. № 6 (34). P. 17–36.

7. Dichenko S.A., Finko O.A. Reduced input redundancy while providing the stability of information-analytical systems in compensating the effects caused by attacker's destructive actions. Automation of Control Processes. 2020. № 4 (62). P. 38–48.

8. Dichenko S.A., Finko O.A. Control and restoration of data integrity in protected information and analytical systems. Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2021. № 676. P. 36–49.

9. Viktorov E.A., Ivanin A.N., Kanaev A.K. Methodology for ensuring the stability of the functioning of a special-purpose transport communication network in the conditions of network and computer attacks. Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2020. № 672. P. 92–101.