УДК 004.056.5

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АСУ ВОЕННОГО НАЗНАЧЕНИЯ

С.Г. КРАСНОВ, адъюнкт

Военная академия воздушно-космической обороны
имени Маршала Советского Союза Г.К. Жукова,
170003, Тверь, ул. Жигарева, д. 50, e-mail: garvel568@yandex.ru

Рассматривается классификация угроз безопасности информации. Приведены наиболее вероятные угрозы, которые могут быть применены противником к автоматизированным системам управления военного назначения, а также рассмотрены возможные последствия.

Ключевые слова: информационная безопасность, угрозы безопасности информации, АСУ военного назначения, защита информации, несанкционированный доступ, несанкционированные воздействия, компьютерные атаки.

DOI: 10.46573/2658-5030-2020-4-85-96

ВВЕДЕНИЕ

Непрерывное совершенствование информационных технологий, повышение их роли и значимости, расширение сферы применения автоматизированных систем управления военного и специального назначения (АСУ ВиСН) в процессе управления государством и его Вооруженными силами требуют постоянного внимания к вопросам обеспечения их информационной безопасности.

Обеспечение информационной безопасности АСУ представляет собой комплексную проблему, которая решается в рамках нормативного и правового регулирования применения АСУ, совершенствования методов и средств их разработки, развития системы оценки соответствия требованиям информационной безопасности, обеспечения соответствующих организационно-технических условий безопасности эксплуатации, включая управление системой обеспечения безопасности обрабатываемой информации.

В настоящее время в мире (в том числе в России) разработано множество стандартов, рекомендаций и других нормативных документов, содержащих как методологии управления рисками, так и основные подходы к этому процессу. В соответствии с этими стандартами основой для проведения анализа рисков информационной безопасности и важнейшей стороной определения требований к системе защиты является формирование модели потенциального нарушителя, а также идентификация, анализ и классификация угроз с последующей оценкой степени вероятности их реализации.

Вместе с тем в настоящее время активно развивается широкий спектр новых методов и технологий информационного воздействия как на отдельные элементы вычислительной техники (ВТ), так и на АСУ органов государственного и военного управления с целью получения несанкционированного доступа к информационным ресурсам и нарушения их функциональной устойчивости. Разрабатываются новые информационные технологии для проведения информационных атак на АСУ ВиСН,

постоянно совершенствуются существующие и появляются новые способы и средства проведения атак, а число компьютерных инцидентов ежегодно увеличивается.

Автоматизированная система управления военного и специального назначения рассматривается в качестве одного из приоритетных объектов комплексного деструктивного воздействия, направленного на достижение информационного превосходства и нарушение (затруднение) управления [1], поэтому решение проблемы обеспечения безопасности АС включает в себя определение, анализ и классификацию возможных угроз безопасности АС.

Целью работы является анализ угроз информационной безопасности, характерных для АСУ военного назначения, для определения требований к системе защиты информации и, как следствие, для подготовки и принятия обоснованных решений по защите информации в АСУ военного назначения.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Одним из важнейших аспектов обеспечения информационной безопасности является анализ и классификация потенциальных угроз. Перечень актуальных угроз, оценка вероятности их реализации, а также составление модели и характеристика нарушителя служат основой для проведения анализа рисков и формулирования требований к каждой системе информационной безопасности.

Существует огромное количество определений понятия «угрозы безопасности информации», поэтому для исследования будем пользоваться определением, представленным в [2].

Перечень угроз безопасности информации содержит сотни позиций. Кроме выявления угроз, целесообразно проведение анализа этих угроз путем их классификации по ряду признаков, каждый из которых отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование. Общая классификация угроз представлена на рисунке [3].

Классификация угроз безопасности информации

Поскольку основным классификационным признаком угроз безопасности выступает их направленность, то в соответствии с этим выделяют угрозы нарушения конфиденциальности, целостности и доступности информации.

Угрозы нарушения доступности направлены на создание таких ситуаций, когда действия злоумышленника либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым ресурсам.

К угрозам нарушения доступности в современных образцах военной и специальной техники (ВСТ) относятся:

повторение или замедление элементов протокола;

подавление обмена в телекоммуникационных сетях;

моделирование ложной тождественности узла вычислительной сети или связи для передачи данных;

использование ошибок или недокументированных возможностей служб и протоколов передачи данных для инициирования отказа в обслуживании;

перерасход вычислительных или телекоммуникационных ресурсов.

Угрозы нарушения целостности направлены на изменение или искажение информации, что приводит к нарушению ее качества или полному уничтожению.

К угрозам нарушения целостности информации относятся:

несанкционированная модификация либо удаление программ или данных;

вставка, изменение или удаление данных в элементах протокола в процессе обмена между абонентами вычислительной сети;

потеря данных в результате сбоев, нарушения работоспособности элементов вычислительной сети или некомпетентных действий субъектов доступа.

Сертифицированные средства защиты удаленного доступа – межсетевые экраны – в настоящее время обеспечивают защиту на физическом, канальном, сетевом, транспортном уровнях. Противодействие информационным воздействиям противника функциями межсетевого экрана на сеансовом, представительном и прикладном уровнях не предусматривается, что представляет существенную опасность нарушения устойчивости функционирования АСУ военного назначения. В связи с этим при построении системы комплексной защиты информации необходимо предусматривать меры защиты сетевых программ и протоколов передачи данных на всех уровнях модели ISO/OSI согласно стандарту ISO/IEC 177999 [4].

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной информации. В случае реализации этих угроз информация становится доступной лицам, которые не должны иметь к ней доступа. С точки зрения компьютерной безопасности нарушение конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ (НСД) к некоторой закрытой информации. *К угрозам нарушения конфиденциальности информации относятся:*

несанкционированное чтение или копирование информации, в том числе остаточной или технологической, на любом из этапов ее обработки;

несанкционированный импорт или экспорт конфиденциальной информации;

передача информации между элементами вычислительной сети, относящимся к разным классам защищенности [8].

При этом в качестве объекта угрозы рассматривается как оперативная информация, обрабатываемая в интересах конечных пользователей, так и технологическая, используемая для организации функционирования комплекса средств обработки информации и комплекса средств защиты информации.

Применительно к условиям информационного противоборства термин «защита информации от НСД» включает в себя все аспекты обеспечения безопасности информации:

защиту от несанкционированного чтения или копирования (обеспечение конфиденциальности);

защиту от несанкционированного изменения или удаления (обеспечение целостности);

защиту от несанкционированного блокирования (обеспечение доступности).

Основной формой информационного воздействия нарушителя на ресурсы вычислительной сети являются компьютерные атаки (КА), представляющие собой упорядоченные во времени действия по преодолению системы защиты и нарушению безопасности информации, реализуемые посредством программ с потенциально опасными (деструктивными) функциями. К числу таких функций относятся:

сокрытие признаков своего присутствия в программно-аппаратной или вычислительной сети;

осуществление сбора данных о параметрах вычислительной сети и о системе ее защиты;

самодублирование или перенос своих фрагментов в другие области оперативной или внешней памяти;

ассоциирование с другими программами в вычислительном окружении;

искажение или разрушение кода программ в оперативной памяти;

сохранение фрагментов информации из оперативной памяти в некоторой области внешней памяти (локальной или удаленной);

искажение, блокирование или подмена выводимого во внешнюю память или в каналы связи массива информации, образующейся при выполнении прикладных программ;

подавление информационного обмена в телекоммуникационных сетях;

искажение или фальсификация информации при обмене по каналам телекоммуникационных сетей;

нейтрализация или нарушение работы тестовых программ и системы защиты [5].

В случае успеха КА реализуются одна или несколько угроз безопасности функционирования вычислительной сети, т.е. потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или другие компоненты вычислительной сети могут прямо или косвенно привести к нарушению безопасности информации.

В зависимости от расположения источника угрозы выделяют внутренние и внешние угрозы безопасности. Основным источником внутренних угроз являются квалифицированные специалисты в области разработки и эксплуатации программного обеспечения (ПО) и технических средств, знакомые со спецификой решаемых в АС задач, структурой, основными функциями и принципами работы программно-аппаратных средств защиты информации, имеющие возможность использования штатного оборудования и технических средств сети.

В зависимости от конкретных условий функционирования и особенностей вычислительной системы в качестве внутренних угроз могут выступать:

авторизованные субъекты доступа – администратор вычислительной сети, администратор баз данных, администратор безопасности, пользователи, программисты, разработчики;

вспомогательный технический и обслуживающий персонал – служба охраны, жизнеобеспечения и др.

Источники внешних угроз:

деятельность международных террористических организаций [6];

деятельность космических, воздушных, морских и наземных технических и иных средств разведки иностранных государств [6];

хакеры или недобросовестные поставщики телекоммуникационных услуг [7];

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов страны в информационной сфере [6].

Все существующие на сегодняшний день угрозы безопасности информации АСУ можно разделить на естественные и искусственные. Естественные угрозы безопасности – это угрозы, вызванные физическим воздействием на АСУ и ее элементы стихийных природных явлений, не зависящих от человека. Более широк и опасен круг вызванных человеческой деятельностью искусственных угроз информации в АСУ, среди которых, исходя из мотивов, можно выделить непреднамеренные и преднамеренные. Источником первых могут быть ошибки в ПО, выход из строя аппаратных средств, неправильные действия пользователей или администратора сети и т.п. Преднамеренные угрозы, в отличие от непреднамеренных, преследуют цель нанесения ущерба пользователям (абонентам) сети и в свою очередь подразделяются на активные и пассивные. Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов и не оказывают при этом влияния на функционирование АСУ. Пассивной угрозой может являться, например, попытка получения информации, циркулирующей в каналах передачи данных, посредством прослушивания последних. Активные угрозы имеют цель нарушения нормального воздействия на ее аппаратные, программные и информационные ресурсы. Так, применительно к современным АСУ военного назначения информационное противоборство представляет собой особую форму конфликта с активным воздействием противника и пассивным поведением системы защиты АСУ. В подобных условиях обеспечения безопасности функционирования АСУ предполагает защиту обрабатываемой в ней информации от НСД, а также защиту информации самой АСУ от несанкционированного воздействия (НСВ) со стороны противника, направленного на нарушение ее функционирования.

Защита информации от НСВ – это защита информации, направленная на предотвращение воздействий на защищаемую информацию с нарушением установленных прав и правил на изменение информации и НСД, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [9].

В отдельный класс угроз следует выделить события, которые в зависимости от условий могут нарушить любую из составляющих безопасности информации:

проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

несанкционированное включение в состав комплексов средств обработки информации и средств защиты информации новых элементов или изменение режимов их работы;

доступ к ресурсам вычислительной сети без использования штатных средств вычислительной техники (СВТ) либо выполнение программ или действий в обход системы защиты;

подбор, перехват или разглашение (компрометация) параметров аутентификации или ключей шифрования (дешифрования);

несанкционированный запуск программ;

использование нестойких параметров аутентификации или ключей шифрования либо их несвоевременная смена;

навязывание ранее переданного или ложного сообщения, отрицание факта его передачи или приема;

некомпетентное использование, настройка или администрирование комплексов средств обработки информации и средств защиты информации;

сбои и отказы в работе комплексов средств обработки информации и средств защиты информации.

Анализ угроз информационной безопасности функционирования образцов вооружения, ВСТ в условиях информационной войны [10] позволяет сделать вывод, что в зависимости от текущего уровня защищенности информации от НСВ стратегии нарушителя по преодолению системы защиты будут изменяться.

Реализация противником (нарушителем) вышеперечисленных угроз (даже частичная) может привести к нарушению (снижению эффективности) функционирования соединения ПВО и нанести ущерб, который может быть сопоставим с ущербом от применения возможным противником современных ударных средств поражения и даже превосходить его. Их действие направлено практически против всех структурных компонентов современных систем управления, а их источники могут располагаться как в самой АСУ, так и вне ее, в том числе быть удаленными на значительное расстояние.

В качестве уязвимых мест для НСД к информации, циркулирующей в АСУ военного назначения, и реализации угроз могут выступать:

свободные порты в коммуникационном оборудовании;

сетевые интерфейсы;

незащищенные стеки протоколов передачи данных;

ошибочно реализованные функции общего и специального программного обеспечения и другие нарушения.

Для формирования перечня угроз безопасности используем Банк данных угроз безопасности информации (далее – Банк данных угроз), созданный ФСТЭК России. В настоящее время АСУ военного назначения используют различные системы, преимущественно импортного производства, поэтому содержимое Банка данных угроз позволяет определить наиболее специфичные для данных АСУ угрозы. Данная информация позволяет при оценке рисков информационной безопасности учитывать тот факт, что каждая конкретная угроза воздействует на определенные типы объектов АСУ. Перечень таких угроз представлен в табл. 1.

Таблица 1. Угрозы безопасности информации

Угроза	Описание	Источник	Объект воздействия
1	2	3	4
Угроза изменения компонентов информационной (автоматизированной) системы	Заключается в возможности получения нарушителем доступа к сети, файлам путем несанкционированного изменения состава программных или аппаратных средств системы, что в дальнейшем позволит осуществлять несанкционированные действия. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе	Внутренний нарушитель с низким потенциалом	Информационная система. Автоматизированное рабочее место

Продолжение табл. 1

1	2	3	4
Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Заключается в возможности прохождения нарушителем процедуры авторизации на основе идентификационной и аутентификационной информации, соответствующей учетной записи «по умолчанию». Реализация возможна при наличии у нарушителя сведений о производителе/модели объекта защиты и об идентификационной и аутентификационной информации	Внешний нарушитель с низким потенциалом; внешний нарушитель со средним потенциалом	Средства защиты информации, системное ПО, программно-аппаратные средства со встроенными функциями защиты
Угроза использования слабостей протоколов сетевого/локального обмена данными	Заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защиты информации за счет деструктивного воздействия на протоколы сетевого/локального обмена данными путем нарушения правил использования таких протоколов. Реализация возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	Внутренний нарушитель с низким потенциалом; внешний нарушитель с низким потенциалом	Системное ПО, сетевой трафик, сетевое ПО
Угроза несанкционированного создания учетной записи пользователя	Заключается в возможности создания дополнительной учетной записи пользователя в собственных неправомерных целях. Реализация возможна при наличии прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях	Внутренний нарушитель с низким потенциалом; внешний нарушитель с низким потенциалом	Системное ПО
Угроза обхода некорректно настроенных механизмов аутентификации	Заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации. Реализация возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации	Внутренний нарушитель с низким потенциалом; внешний нарушитель с низким потенциалом	Системное ПО, сетевое ПО
Угроза подмены действий пользователя путем обмана	Заключается в возможности выполнения нарушителем неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии. Реализация возможна при наличии у дискредитируемого пользователя нужных прав	Внешний нарушитель со средним потенциалом	Прикладное ПО; сетевое ПО

Окончание табл. 1

1	2	3	4
Угроза удаления аутентификационной информации	Заключается в возможности отказа легитимным пользователям в доступе к информационным ресурсам	Внутренний нарушитель с низким потенциалом; внешний нарушитель с низким потенциалом	Системное ПО, учетные данные пользователя
Угроза обхода многофакторной аутентификации	Заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в систему и компоненты, участвующие в процедуре многофакторной аутентификации	Внешний нарушитель с высоким потенциалом	Системное ПО, учетные данные пользователя

Полученный перечень угроз не является окончательным и в дальнейшем будет уточняться и дополняться (за счет использования всевозможных сочетаний базовых атрибутов угроз, которые будут определять возможную угрозу безопасности) при построении модели угроз.

Помимо определения перечня угроз, необходимо знать, какие последствия повлечет за собой их реализация. В Банке данных угроз в качестве последствий от реализации угроз рассматривается нарушение тех или иных свойств безопасности информации (конфиденциальности, доступности, целостности). Применительно к АСУ военного назначения наиболее критичными являются нарушения, влекущие за собой негативные последствия для функционирования системы управления в целом. Для того чтобы определить возможные последствия каждой угрозы, следует опираться на информацию о функциональном назначении объекта воздействия угрозы или подсистемы, в которую он входит. Это важно, так как последствия от одной и той же угрозы, реализованной в отношении разных компонентов системы управления, могут различаться в зависимости от критичности выполняемых функций каждого компонента.

Возможные последствия нарушения функционирования АСУ военного назначения в результате реализации угроз информационной безопасности представлены в табл. 2.

Таблица 2. Возможные последствия нарушения функционирования АСУ

Объект воздействия	Последствия
1	2
Пункты управления	Нарушение выполнения (снижение качества выполнения) планов работ по объектам управления. *Способы воздействия*: программно-аппаратные воздействия на средства локальных вычислительных сетей (ЛВС), разрабатываемые по технологии «Intranet» и IP телефонии; ввод ложных данных; сбор некачественной (ложной) информации; несанкционированные подключения внешних абонентов к серверам баз данных; воздействия компьютерных вирусов; проявление НДВ и НСВ

Продолжение табл. 2

1	2
Объекты управления	Комплексное нарушение процессов управления и нештатное функционирование АСУ, потеря актуальной управляющей информации. *Способы воздействия*: программно-аппаратные воздействия ЛВС, искажение данных, несанкционированные подключения внешних абонентов к пунктам управления, разрыв соединения между абонентами, воздействия компьютерных вирусов
Потребители информации	Не выполняются целевые задачи информационного обеспечения и вследствие этого снижение эффективности управления. *Способы воздействия*: косвенные воздействия на АСУ. В случае несанкционированного подключения к средствам обработки информации создаются дополнительные предпосылки для реализации КА, воздействия компьютерных вирусов, проявления НДВ и НСВ
Территориально-распределенные вычислительные сети, ЛВС	Нарушение информационно-логического взаимодействия абонентов, функций мониторинга сети, электронной почты и протоколов передачи данных. *Способы воздействия*: искажение, блокирование, уничтожение пакетов данных, нарушение адресации и порядка администрирования сети, настройка ложной маршрутизации пакетов данных при недостаточной защите удаленного доступа межсетевыми экранами; отсутствие средств предупреждения и обнаружения КА, возможностей НСВ на информацию и проявления НДВ, проникновения компьютерных вирусов
Сетевые операционные системы	Нарушение информационно-вычислительного процесса в КТС АСУ и прав доступа к информационным ресурсам операционной системы (ОС). *Способы воздействия*: программно-аппаратные воздействия на системные файлы и регистры ОС; несанкционированные перезапуски «зависание» ОС, взлом программ разграничения доступа операторов к информации при недостаточно эффективной работе встроенных средств защиты от НСВ и администрирования ОС, программного межсетевого экрана, антивирусных средств, проявления НДВ (датчика ОС – при установке средств противодействия информационным угрозам)
Система управления базами данных (СУБД) и базы данных (БД)	Нарушение целостности и доступности данных в результате искажения информационных таблиц и правил доступа к информационным ресурсам СУБД. *Способы воздействия*: ввод ложных данных, искажение алгоритмов обработки транзакций, нарушение структуры интерфейсов и целостности БД, создание условий для противоречивости предоставляемых данных вследствие воздействия атак, НСВ на информацию, наличие уязвимых мест в средствах защиты СУБД, БД и НДВ в ее программах при отсутствии средств противодействия КА в серверах сбора информации

Окончание табл. 2

1	2
Специальное программное обеспечение (СПО), комплексы расчетных программ	Нарушение точности и достоверности данных, необходимых для выполнения арифметическо-логических операций в КТС и прав доступа к СПО; невыполнение (несвоевременное выполнение) требуемого объема вычислительных операций. *Способы воздействия*: ввод ложных данных, блокирование, остановка выполнения программ, искажение входных данных и результатов расчета, инициализация ложных событий реконфигурации КВИС при наличии в ПО ошибок и НДВ

При анализе возможных последствий необходимо учитывать, что некоторые угрозы не приводят к каким-либо последствиям, но они могут повлечь реализацию других угроз, которые уже напрямую влияют на работоспособность системы в целом и выполнение поставленной задачи.

ЗАКЛЮЧЕНИЕ

Анализ угроз информационной безопасности показывает, что потенциальные угрозы информации в современных АСУ военного назначения отличаются многообразием и сложностью структуры. Их действие направлено практически против всех структурных компонентов современных систем управления, а их источники могут располагаться как в самой АСУ, так и вне ее, в том числе на значительном расстоянии.

Для определения ущерба информации должны быть разработаны соответствующие методы и модели, учитывающие степень опасности всех угроз в их совокупности при существующих технологиях построения и функционирования АСУ военного назначения. Постоянное совершенствование существующих и появление новых угроз информационной безопасности приводит к невозможности рассмотрения каждой угрозы в отдельности, поэтому необходима их классификация. Оценка степени опасности угроз может быть выполнена на основе разработки моделей возможных действий нарушителя по их реализации.

Таким образом, в условиях реализации противником информационных угроз существует реальная опасность нарушения функционирования элементов АСУ. Это может привести к невыполнению возложенных на данную автоматизированную систему задач и, как следствие, к потере управления подчиненными силами и средствами, что в конечном счете может негативно повлиять на эффективность выполнения боевой задачи.

ЛИТЕРАТУРА

1. Бородакий Ю.В., Добродеев А.Ю., Нащекин П.А., Бутусов И.В. О подходах к реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения // *Вопросы кибербезопасности*. 2014. № 2 (3). С. 2–9.

2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: Стандартиформ, 2009. 16 с.

3. Галатенко В.А. Основы информационной безопасности: курс лекций, учебное пособие / под ред. В.Б. Бетелина. М.: Интернет-университет информационных технологий, 2006. 208 с.

4. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management. Berlin: Deutsches Institut für Normung, 2005. 129 p.

5. Барнс К., Боутс Т., Ллойд Д. [и др.]. Защита от хакеров беспроводных сетей / пер. с англ. А.В. Семенова. М.: Компания АйТи, ДМК Пресс, 2005. 476 с.

6. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 9 сентября 2000 г. № 1895. URL: https: //base.garant.ru/182535/ (дата обращения: 29.08.2020).

7. Ахмад Д.М., Дубравский И., Флинн Х. [и др.]. Защита от хакеров корпоративных сетей. М.: Компания АйТи, ДМК Пресс, 2005. 864 с.

8. Митюшов Д.Г., Перепелица С.В. Анализ современных средств и методов защиты информационных ресурсов АСУ ВКО от НСВ // Научно-методический сборник № 41. Тверь: ВА ВКО, 2011.

9. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М.: Госстандарт России, 1996. 8 с.

10. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. 368 с.

Для цитирования: Краснов С.Г. Анализ современных угроз безопасности информации в АСУ военного назначения // Вестник Тверского государственного технического университета. Серия «Технические науки». 2020. № 4 (8). С. 85–96.

ANALYSIS OF MODERN THREATS TO INFORMATION SECURITY IN A MILITARY AUTOMATED CONTROL SYSTEM

S.G. KRASNOV, Adjunct

Military Academy of Aerospace Defense named after Marshal of the Soviet Union G.K. Zhukov, 50, Zhigareva st., 170003, Tver, Russian Federation,
e-mail: garvel568@yandex.ru

It is considered the classification of threats to information security, presents the most likely threats that can be applied by the enemy to automated control systems for military purposes, and the possible consequences that can occur in this case.

Keywords: information security, threats to information security, military automated control systems, information protection, unauthorized access, unauthorized impacts, computer attacks.

REFERENCES

1. Borodakiy Yu.V., Dobrodeev A.Yu., Naschekin P.A., Butusov I.V. On approaches to the implementation of a centralized system of information security management ACS military and special purpose. *Voprosy kiberbezopasnosti*. 2014. № 2 (3), pp. 2–9. (In Russian).

2. GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. Moscow: Standardinform, 2009. 16 p.

3. Galatenko V.A. Osnovy informatsionnoy bezopasnosti: kurs lektsiy, uchebnoye posobiye / pod red. V.B. Betelina. [Information security basics: a course of lectures, a textbook; ed. V.B. Betelina]. Moscow: Internet-universitet informatsionnykh tekhnologiy, 2006. 208 p.

4. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management, Berlin: Deutsches Institut für Normung. 2005. 129 p.

5. Barns K., Bouts T., Lloyd D. et al. Zashchita ot khakerov besprovodnykh setey / per. s angl. A.V. Semenova. [Protection against hackers of wireless networks. Per. from English. A.V. Semenov]. Moscow: Kompaniya AyTi, DMK Press, 2005. 476 p.

6. Doctrine of information security of the Russian Federation: Decree of the President of the Russian Federation dated September 09, 2000 No. 1895. URL: https://base.garant.ru/182535/ (data accessed: 29.08.2020). (In Russian).

7. Akhmad D.M., Dubravskiy I., Flinn KH. [et al.]. Zashchita ot khakerov korporativnykh setey. [Protection from hackers of corporate networks]. Moscow: Kompaniya AyTi, DMK Press. 2005. 864 p.

8. Mityushov D.G., Perepelitsa S.V. Analysis of modern means and methods of protecting information resources of ACS VKO from NSV. *Nauchno-metodicheskiy sbornik № 41.* Tver: VA VKO. 2011. (In Russian).

9. GOST R 50922-96. The protection of information. Basic terms and definitions. Moscow: Gosstandart Rossii, 1996. 8 p.

10. Melnikov V.V. Bezopasnost informatsii v avtomatizirovannykh sistemakh. [Security of information in automated systems]. Moscow: Finansy i statistika, 2003. 368 p.

Поступила в редакцию/received: 02.07.2020; после рецензирования/revised: 25.08.2020; принята/accepted 17.09.2020