Министерство внутренних дел Российской Федерации
Казанский юридический институт

А.М. Каримов, С.В. Смирнов, Г.Д. Марданов

Основы кибербезопасности

Казань
КЮИ МВД России
2022

ББК 32.85 + 16.82 + 74.263.2
К23

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:
кандидат экономических наук **М.Н. Трофимов**
(Рязанский филиал Московского университета
МВД России им. В.Я. Кикотя);
кандидат юридических наук **В.В. Кулажников**
(Владивостокский филиал
Дальневосточного юридического института МВД России)

Авторский вклад:
А.М. Каримов – глава 1, глава 2, общая редакция, введение, заключение;
С.В. Смирнов – глава 3, глава 4, перечень практических заданий;
Г.Д. Марданов – глава 5, перечень тестовых вопросов.

К23 **Каримов А.М.**
Основы кибербезопасности: учебно-практическое пособие/ А.М. Каримов, С.В. Смирнов, Г.Д. Марданов. – Казань: КЮИ МВД России. – 63 с.

Учебно-практическое пособие содержит теоретические основы учебной дисциплины «Основы кибербезопасности», практические задания, тестовые вопросы.

Предназначено для преподавателей, курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ББК 32.85 + 16.82 + 74.263.2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» устанавливает, что «полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети «Интернет», автоматизированных информационных систем, интегрированных банков данных»[1]. Органы внутренних дел в своей оперативно-служебной деятельности активно используют информационно-телекоммуникационнные технологии, в частности интегрированную мультисервисную телекоммуникационную систему (ИМТС), предназначенную для передачи масштабных пакетов данных между подразделениями органов внутренних дел Российской Федерации и иными правоохранительными органами, органами государственной и муниципальной власти, общественными объединениями и организациями по защищенным каналам связи. Также полиция в целях выполнения возложенных на нее государством задач вправе собирать данные о гражданах и обобщать эти базы данных в информационных системах. Это право обусловливает обязанность полиции обеспечить защиту таких баз данных в ведомственных информационных системах

Для эффективного выполнения возложенных на органы внутренних дел Российской Федерации задач сотрудники подразделений должны хорошо знать и правильно понимать вопросы обеспечения кибербезопасности в организации. Надёжное обеспечение защиты информации может быть достигнуто только при выстраивании эшелонированных рубежей информационной безопасности. Знание правовых, организационных, технических,

[1] О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ // Доступ из СПС «КонсультантПлюс» (дата обращения: 15.11.2021).

физических, программных и криптографических мер защиты информации требуется и при выполнении общих и специфических функций, так как в процессе их реализации приходится сталкиваться со многими областями сложных, комплексных решений, разобраться в которых и сделать правильные выводы можно только при хорошем знании данного направления деятельности.

Настоящее учебно-практическое пособие посвящено вопросам обеспечения кибербезопасности в органах внутренних дел Российской Федерации. В пособии наглядно изложены общие вопросы, нормативно-правовое обеспечение кибербезопасности, угрозы информационной безопасности ОВД РФ, меры противодействия угрозам кибербезопасности, вредоносные программы как угроза информационной безопасности и антивирусные программы как средства противодействия этим угрозам, подробно освещены актуальные подходы к защите информации.

ГЛАВА 1.
ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Рис. 1

Компьютерная информация – «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[1].

Для компьютерной информации свойственны определенные черты, которые определяют характерные особенности деятельности с электронными носителями информации (рис. 1):

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.11.2022).

Информационная безопасность – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от государственного сектора до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Безопасность сетей – действия по защите компьютерных сетей от различных угроз, например, целевых атак или вредоносных программ.

Безопасность приложений – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.

Безопасность информации – обеспечение целостности и приватности данных как во время хранения, так и при передаче.

Операционная безопасность – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.

В действительности эти термины сильно различаются и не являются взаимозаменяемыми. Под **кибербезопасностью** понима-

ют защиту от атак в киберпространстве, а под **информационной** безопасностью – защиту данных от любых форм угроз, независимо от того, являются ли они аналоговыми или цифровыми (рис. 2).

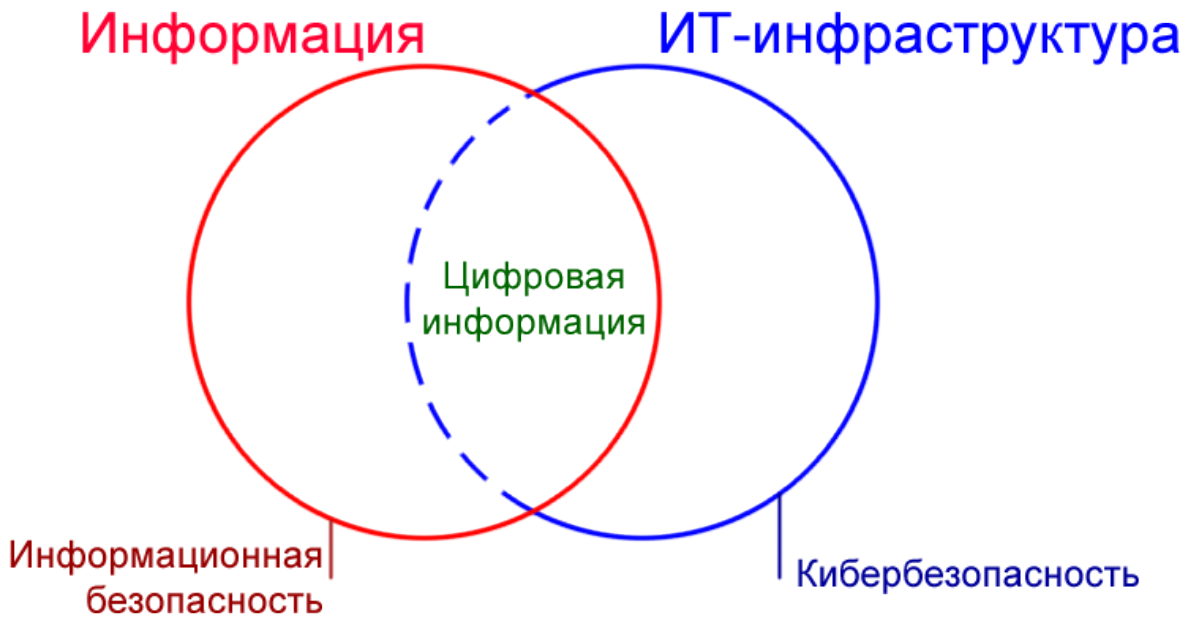

Рис. 2

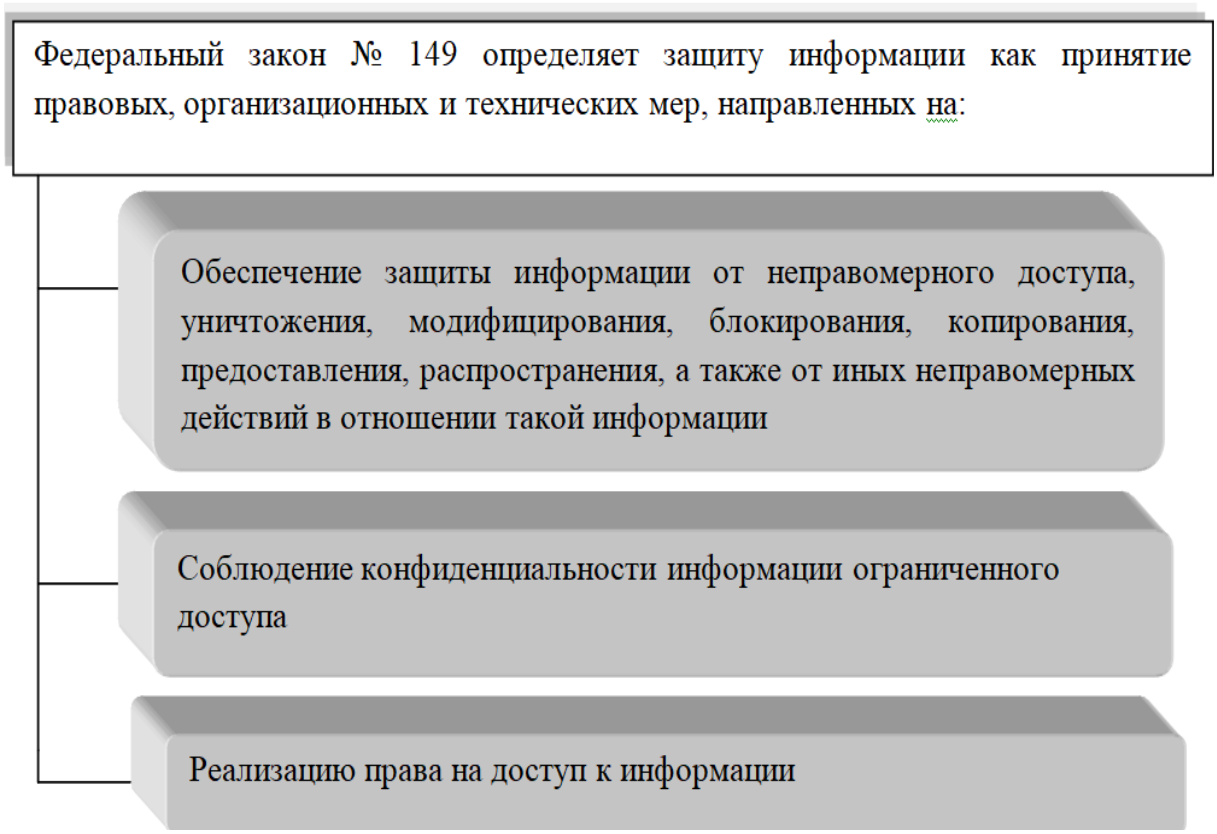

Рис. 3

Защита информации – представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации (рис. 3).

Безопасность информационной системы – это свойство, заключающееся в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации.

Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Под целостностью понимается невозможность несанкционированного или случайного уничтожения, а также модификации информации.

Под конфиденциальностью информации – невозможность утечки и несанкционированного завладения хранящейся, передаваемой или принимаемой информации (рис. 4).

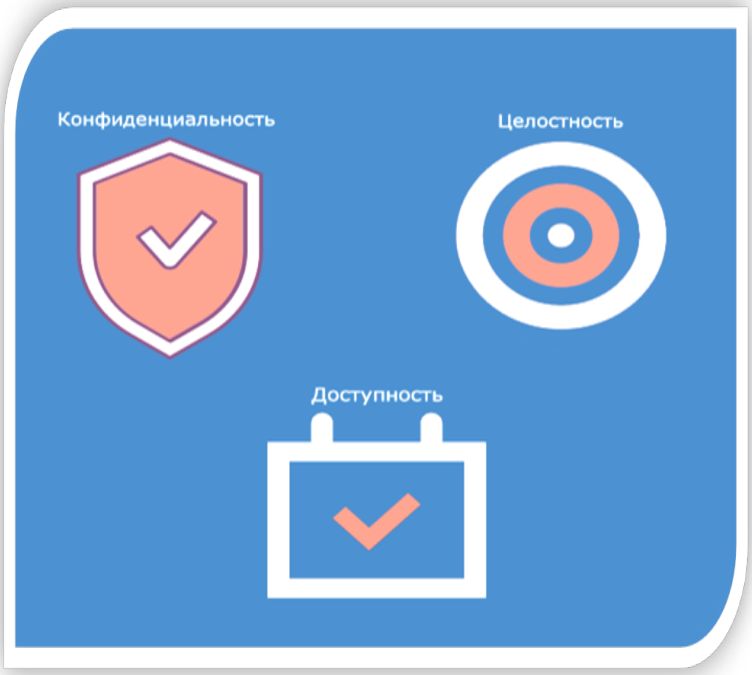

Рис. 4

К ведомственным объектам критической инфраструктуры относятся (рис. 5):

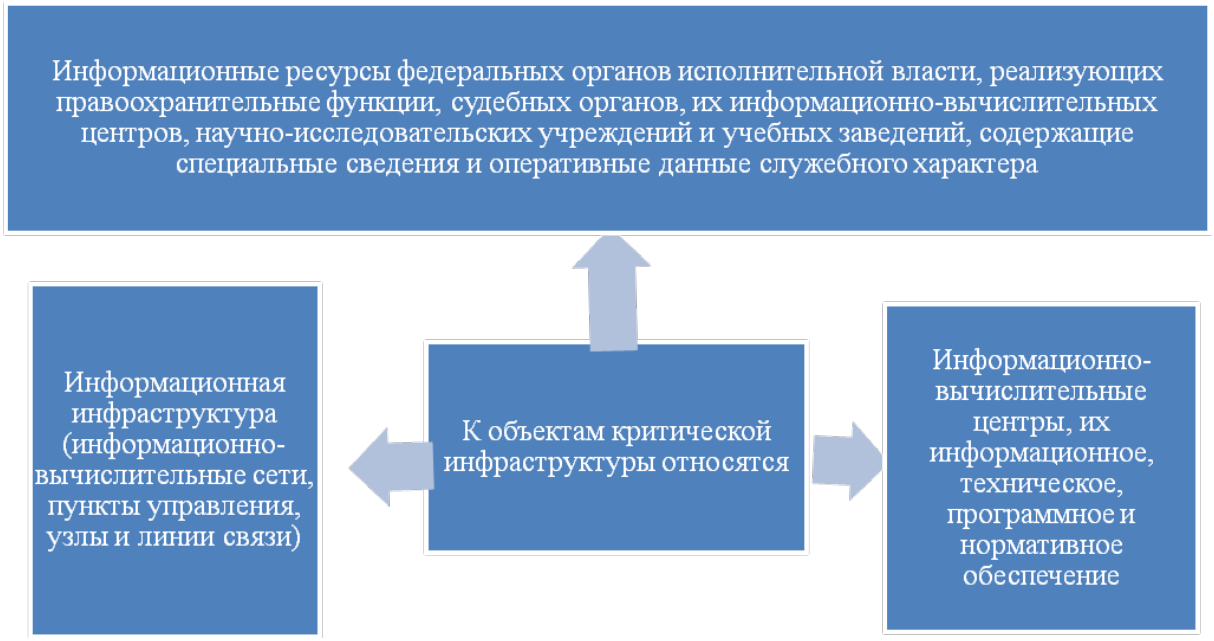

Рис. 5

К разновидностям конфиденциальной компьютерной информации, подверженной угрозам информационной безопасности в органах внутренних дел Российской Федерации, можно отнести следующее (рис. 6):

Рис. 6

1) персональные данные граждан (самый масштабный класс конфиденциальной информации, а органы внутренних дел Российской Федерации – самый масштабный оператор этих персональных данных);

2) государственная тайна (самый опасный, с точки зрения последствий, от возможного несанкционированного доступа и распространения класс конфиденциальной информации, предусматривающей самые жесткие санкции (уголовную ответственность) за неправомерный доступ);

3) тайна следствия и судопроизводства;

4) несекретная информация ограниченного распространения (служебная тайна), ограничения на распространение которых диктуются положениями приказа МВД России от 09.11.2018 № 755.

ГЛАВА 2.
НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Основными нормативно-правовыми актами, регулирующими общественные отношения в сфере обеспечения кибербезопасности в Российской Федерации в целом и в ОВД РФ в частности, являются (рис. 7):

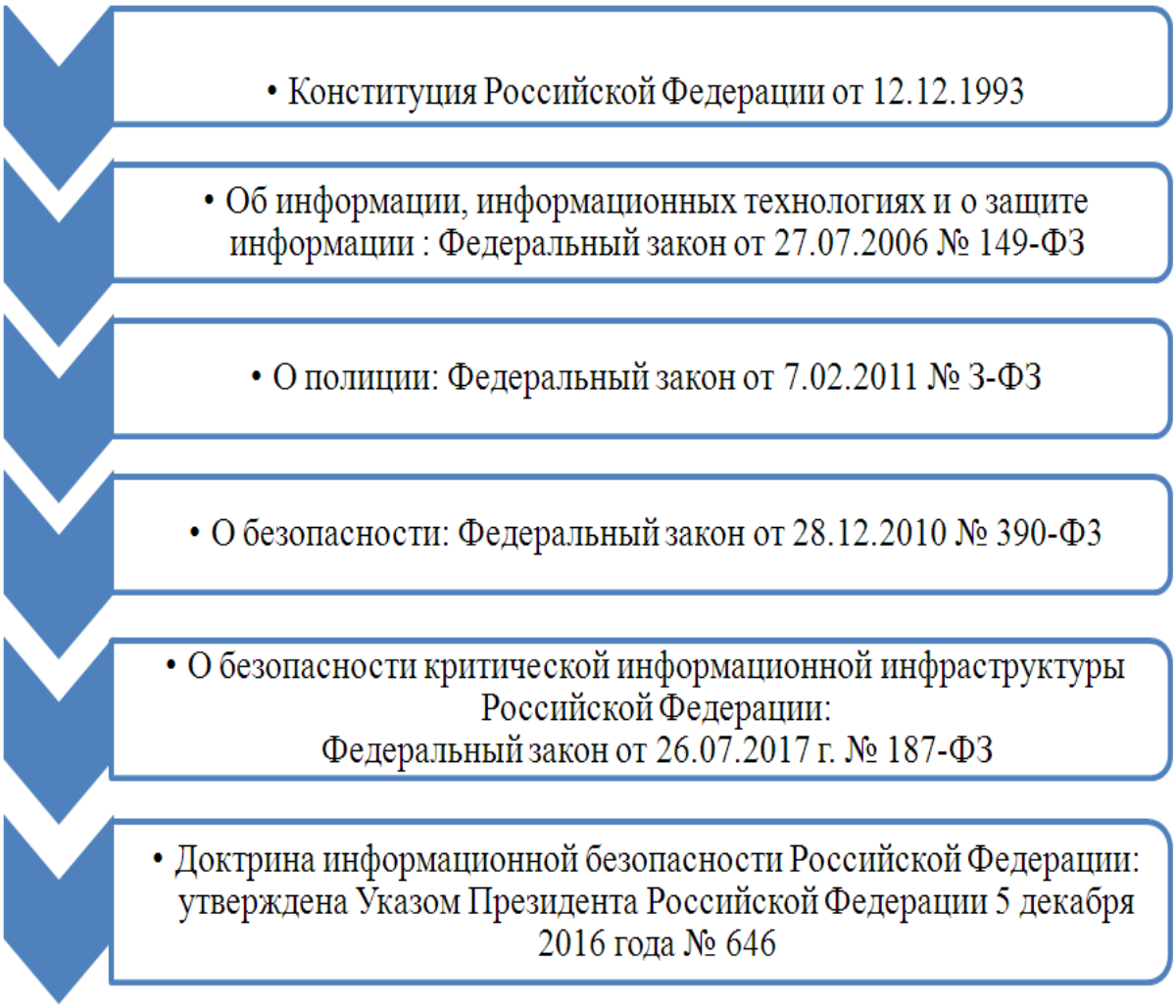

Рис. 7

Конституция Российской Федерации провозглашает следующее: право каждого гражданина свободно искать, получать, пе-

редавать, производить и распространять информацию любым законным способом (ст. 29, п. 4): гарантируется свобода массовой информации и запрещается ее цензура (ст. 29, п. 5); каждый гражданин наделяется правом на неприкосновенность частной жизни, сохранность личной и семейной тайны (ст. 23, п. 1); сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24, п. 1); согласно Конституции, каждому гарантируется свобода мысли и слова

Рис. 8

(ст. 29, п. 1), а также свобода литературного, художественного, научного, технического и других видов творчества (ст. 44, п. 1) (рис. 8).

Основным нормативно-правовым актом в области защиты информации является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149). Упомянутый федеральный закон в первую очередь отграничивает информацию свободно распространяемую, а также информацию ограниченного доступа. В статье 5 документа указано, что доступ к информации может быть ограничен только федеральными законами. Также ФЗ № 149 содержит в себе правовые термины в области информационной безопасности и технологий, а также юридические принципы регулирования отношений в разнообразных областях информационных взаимоотношений, в том числе защиты информации.

Директивные задачи внутренней и внешней политики государства по обеспечению информационной безопасности определяются на основе национальных интересов Российской Федерации в информационной сфере, названные в Доктрине информационной безопасности Российской Федерации, утвержденной указом президента Российской Федерации от 05.12.2016[1] (рис. 9):

1) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий;

2) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры в мирное время, в период непосредственной угрозы агрессии и в военное время;

3) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;

4) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире;

[1] Доктрина информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства Российской Федерации, № 50, 12.12.2016, ст. 7074.

Рис. 9

5) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности (рис. 9).

Основные составляющие национальных интересов Российской Федерации в информационной сфере представлены на рис. 10.


Защита информационных ресурсов от несанкционированного доступа
Обеспечение безопасности информационных и телекоммуникационных систем (уже развернутых, и создаваемых на территории России)
Основные составляющие национальных интересов РФ в информационной сфере

Рис. 10

ГЛАВА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Угрозы информационной безопасности органов внутренних дел Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Безопасность информационных ресурсов и информационной инфраструктуры органов внутренних дел выражается через безопасность их наиболее важных свойств. Так как субъектам информационных отношений урон может быть причинен воздействием на процессы и средства обработки критичной для них информации, то полной необходимостью становится обеспечение защиты всей системы информации от незаконного вторжения, способов хищения и/или разрушения любых компонентов данной системы в процессе ее деятельности.

Известны следующие источники угроз безопасности информационных систем:

- антропогенные источники, вызванные случайными или преднамеренными действиями субъектов;
- техногенные источники, приводящие к отказам и сбоям технических и программных средств из-за устаревших программных и аппаратных средств или ошибок в программном обеспечении;
- стихийные источники, вызванные природными катаклизмами или форс-мажорными обстоятельствами.

Антропогенные источники угроз делятся:

- на внутренние (воздействия со стороны сотрудников компа-

нии) и внешние (несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения) источники;

- на непреднамеренные (случайные) и преднамеренные действия субъектов.

Внутренние угрозы:

- неквалифицированная внутренняя политика;
- отсутствие соответствующей квалификации персонала;
- преднамеренные и непреднамеренные действия персонала по нарушению безопасности;
- техногенные аварии и разрушения, пожары.

Внешние угрозы:

- воздействия недобросовестных конкурентов;
- преднамеренные и непреднамеренные действия заинтересованных лиц и структур;
- утечка конфиденциальной информации;
- несанкционированное проникновение на объект защиты;
- несанкционированный доступ к носителям информации и каналам связи;
- стихийные бедствия;
- преднамеренные и непреднамеренные действия поставщиков услуг по обеспечению безопасности.

Случайные угрозы – угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными. При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Преднамеренные угрозы. Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы

и средства шпионажа и диверсий, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих компьютерных систем (далее – КС). Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К случайным угрозам относятся:

- стихийные бедствия, аварии;
- сбои и отказы технических средств;
- ошибки при разработке компьютерных систем;
- алгоритмические и программные ошибки;
- ошибки пользователей и обслуживающего персонала.

К преднамеренным угрозам относятся:

- традиционный шпионаж и диверсии;
- несанкционированный доступ к информации (НСД);
- электромагнитные излучения и наводки (ПЭМИН);
- несанкционированная модификация структур;
- вредоносное программное обеспечение (вирусы).

Существует много возможных направлений утечки информации и путей несанкционированного доступа к ней в системах и сетях:

▪ перехват информации;

▪ модификация информации (исходное сообщение или документ изменяется или подменяется другим и отсылается адресату);

▪ подмена авторства информации (кто-то может послать письмо или документ от вашего имени);

▪ использование недостатков операционных систем и прикладных программных средств;

▪ копирование носителей информации и файлов с преодолением мер защиты;

▪ незаконное подключение к аппаратуре и линиям связи;

▪ маскировка под зарегистрированного пользователя и присвоение его полномочий;

Соотношение внешних и внутренних угроз (рис. 11):

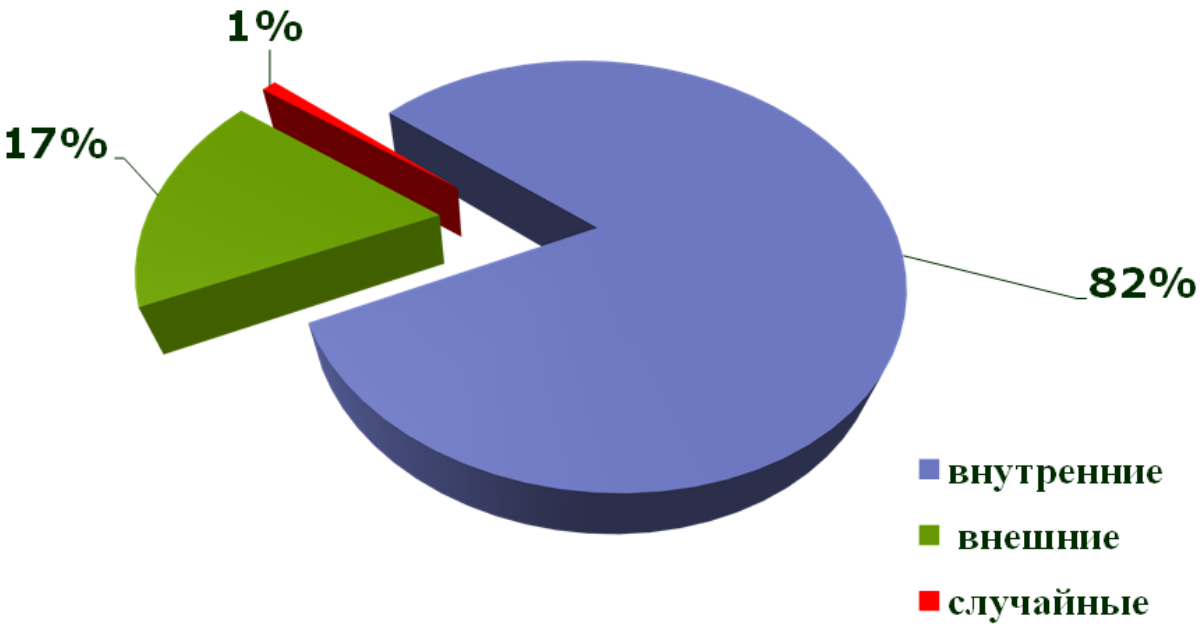

Рис. 11

Минимальные требования информационной безопасности (рис. 12):

Рис. 12

▪ введение новых пользователей;
▪ внедрение компьютерных вирусов и так далее.

Для обеспечения безопасности информационных систем применяются системы защиты информации, которые представляют собой комплекс организационно-технологических мер, программно-технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

При комплексном подходе методы противодействия угрозам интегрируются, создавая архитектуру безопасности систем. Необходимо отметить, что любая системы защиты информации не является полностью безопасной. Всегда приходится выбирать между уровнем защиты и эффективностью работы информационных систем.

К средствам защиты информации информационных систем (далее – ИС) от действий субъектов относятся:

- средства защиты информации от несанкционированного доступа;
- защита информации в компьютерных сетях;
- криптографическая защита информации;
- электронная цифровая подпись;
- защита информации от компьютерных вирусов.

ГЛАВА 4.
МЕРЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ КИБЕРБЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Средства обеспечения информационной безопасности – средства, используемые силами обеспечения информационной безопасности.

К ним относятся:
- технические (физические);
- организационные;
- правовые;
- технологические;
- программные.

Технические меры:
- защита от несанкционированного доступа к системе;
- резервирование особо важных компьютерных подсистем;
- организация вычислительных сетей;
- установка противопожарного оборудования;
- оснащение замками, сигнализациями.

Организационные меры:
- охрана вычислительного центра;
- тщательный подбор персонала;
- наличие плана восстановления работоспособности (после выхода из строя);
- универсальность средств защиты от всех пользователей.

Организационные методы включают в себя три составляющие:

- ограничение доступа;
- разграничение доступа;
- контроль доступа.

Ограничение доступа – это создание некоторых замкнутых рубежей вокруг объекта защиты. Доступ лиц к объекту осуществляется в контролируемых условиях и лишь для выполнения ими функциональных обязанностей. Ограничение доступа в отношении компьютерной системы заключается в исключении доступа к ней посторонних лиц: следует разместить компьютеризированное рабочее место в отдельном изолированном помещении, дверь в помещение должна быть оборудована механическим или электромеханическим замком. В период длительного отсутствия пользователя системный блок и носители информации могут быть изолированы в сейфе.

Разграничения доступа – разделение информации на части и организации доступа к ней в соответствии с функциональными обязанностями пользователя.

Задача разграничения доступа состоит в защите информации от нарушителя, который входит в круг лиц, допущенных к работе в компьютерной системе. При этом деление информации может выполняться в соответствии с различными критериями: по степени важности, секретности, функциональному назначению и т.д. Обычно при организации разграничения доступа следует придерживаться следующих правил: техническое обслуживание оборудования в процессе эксплуатации должно выполняться специальным персоналом без доступа к информации, подлежащей защите; любое изменение программного обеспечения должен выполнять выделенный специально для этой цели специалист.

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: идентификация, аутентификация и авторизация.

Идентификация – присвоение субъекту уникального образа, имени или числа.

Аутентификация – установление подлинности субъекта, то есть происходит процесс проверки, является ли субъект тем, за кого себя выдает.

Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.

Авторизация – проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними. Авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам.

Правовые меры:

Схема процедуры идентификации и аутентификации пользователя безопасности (рис. 13):

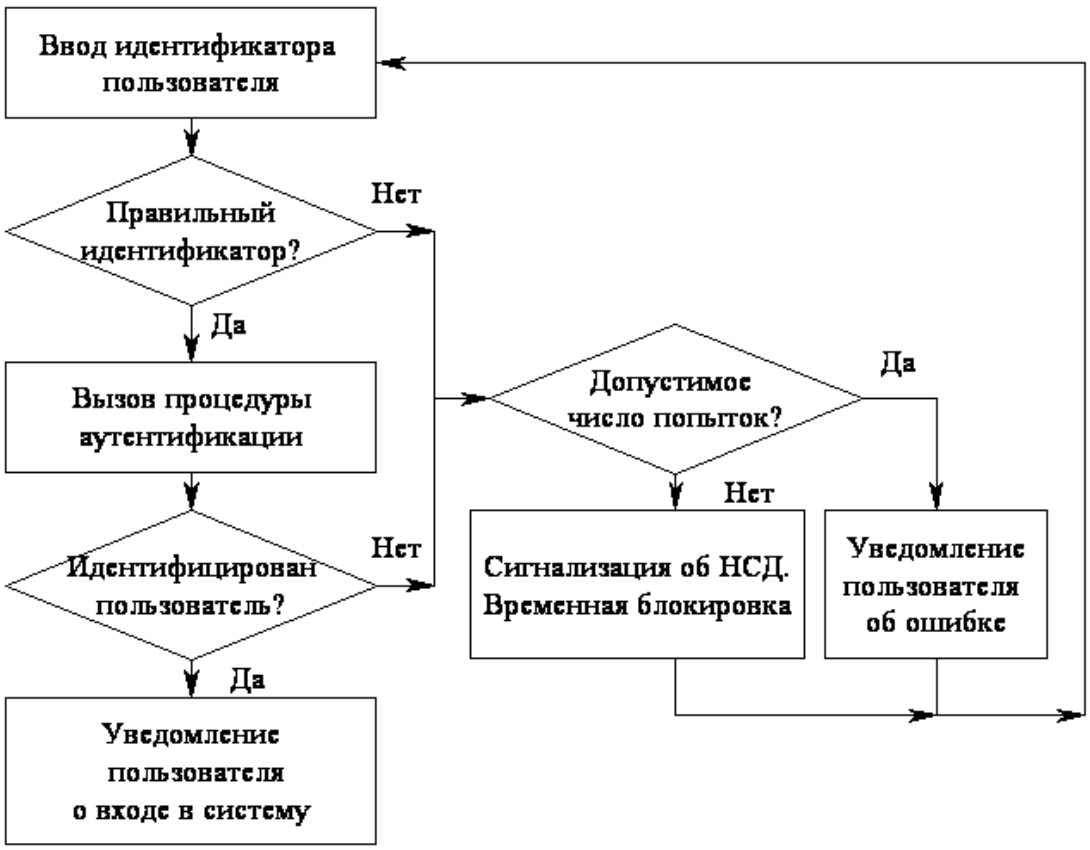

Рис. 13

√ разработка норм, устанавливающих ответственность за преступления в сфере компьютерной информации, а также за преступления, совершаемые с использованием информационно-коммуникационных технологий;

√ издание локальных правовых актов;

√ совершенствование уголовного и гражданского законодательства.

Программные методы защиты данных.

В крупных локальных сетях не так уж редки случаи заражения отдельных компьютеров или целой группы компьютеров различными вирусами. Наиболее распространенными методами защиты от вирусов по сей день остаются всевозможные антивирусные программы.

Однако все чаще и чаще защита с помощью антивирусных программ становится недостаточно эффективной. В связи с этим распространение получают программно-аппаратные методы защиты (сетевые адаптеры Ethernet в Flash-памяти содержат антивирусную программу).

Структурная схема реализации защиты информации (рис. 14):

Рис. 14

ГЛАВА 5. ВРЕДОНОСНЫЕ ПРОГРАММЫ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АНТИВИРУСНЫЕ ПРОГРАММЫ КАК СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ЭТИМ УГРОЗАМ

Вредоносные программы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромным ущербом, наносимым информационным системам.

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей.

Термин *«компьютерный вирус»* появился в середине 1980-х гг., на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла. Согласно современной классификации Лаборатории Касперского, в настоящее время используется более широкое понятие – *«вредоносные программы»,* включающее компьютерные вирусы, сетевые черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью

изменить или уничтожить программное обеспечение и/ или данные, хранящиеся в автоматизированных системах.

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от «вирусов», что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения, до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние «вирусописателей» и их оппонентов будет постоянным.

Классификация вредоносного программного обеспечения.

Сетевые черви представляют собой программы, распространяющие свои копии по локальным и/ или глобальным сетям в целях:

- проникновения на удаленные устройства (компьютеры, мобильные телефоны);
- запуска своей копии на удаленном устройстве;
- дальнейшего перехода на другие устройства в сети.

Пути распространения большинства известных червей следующие:

- вложение в электронное письмо;
- ссылка в ICQ- и IRC-сообщениях на зараженный файл, расположенный на каком-либо веб- или FTP-ресурсе;
- файл в каталоге обмена P2P и др.

Классические компьютерные вирусы – это программы, распространяющие свои копии по ресурсам локального компьютера в целях:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевые сервисы для проникновения в другие компьютеры. Копия вируса попадает на удаленные компьютеры только в тех случаях, если зараженный объект по каким-либо не зависящим от функционала вируса при-

чинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съемный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например шпионскую процедуру или троянский компонент уничтожения информации на диске (например, вирус CIH).

Троянские программы – это вредоносные программы, созданные для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения. Основным признаком, по которому различают типы троянских программ, являются их несанкционированные пользователем действия – те, которые они производят на зараженном компьютере.

Хакерские утилиты и прочие вредоносные программы включают:

▪ утилиты, автоматизирующие создание вирусов, червей и троянских программ (конструкторы);

▪ программные библиотеки, разработанные для создания вредоносных программ;

▪ хакерские утилиты, скрывающие код зараженных файлов от антивирусной проверки (шифровальщики файлов);

▪ «злые шутки», затрудняющие работу с компьютером;

▪ программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;

▪ прочие программы, тем или иным способом намеренно нано-

сящие прямой или косвенный ущерб данному компьютеру или удаленным компьютерам сети.

Классификация вирусов.

Вирусы принято классифицировать по следующим признакам:

- среда обитания;
- особенности алгоритма работы;
- деструктивные возможности.

По алгоритмам работы выделяют резидентные вирусы и вирусы, использующие стелс-алгоритмы или полиморфичность.

Резидентные вирусы при заражении компьютера постоянно остаются в оперативной памяти, перехватывая обращения операционной системы к объектам заражения, чтобы выполнить несанкционированные действия. Такие вирусы являются активными до полного выключения компьютера.

Применение стелс-алгоритмов базируется на перехвате запросов ОС на чтение или запись зараженных объектов. При этом происходит временное лечение этих объектов либо замена их незараженными участками информации. Это позволяет вирусам скрыть себя в системе.

Также очень сложно обнаружить в системе вирусы, основанные на применении алгоритмов полиморфичности. Такие вирусы не содержат ни одного постоянного участка кода, что достигается за счет шифрования кода вируса и модификации программы-расшифровщика. Как правило, два образца одного и того же вируса не будут иметь ни одного совпадения в коде.

По деструктивным, то есть разрушительным возможностям выделяют опасные и неопасные вирусы.

Опасные вирусы выводят из строя операционную систему, портят или уничтожают информацию, хранящуюся на диске.

Неопасные вирусы практически не влияют на работоспособность компьютера и не понижают эффективность работы операционной системы, кроме увеличения дискового пространства, которое они занимают, и уменьшения объёма свободной памяти компьютера.

По особенностям алгоритма работы выделяют:

Паразитические – все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы, которые не являются вирусами-спутниками и вирусами червями.

Стелс-вирусы (вирусы-невидимки, stealth) – представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков, подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

Полиморфные (самошифрующиеся или вирусы-призраки, polymorphic) – вирусы, достаточно трудно обнаруживаемые, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

По среде обитания различают типы компьютерных вирусов: *загрузочные, файловые, макровирусы* и *сетевые.*

Загрузочные вирусы заражают загрузочный сектор гибкого диска или винчестера. При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске отдать управление не программному коду загрузчика операционной системы, а коду вируса.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему операционной системы. Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).

Практически все загрузочные и файловые вирусы *резидентны*, то есть они находятся в оперативной памяти компьютера и в процессе работы пользователя могут осуществлять опасные действия (стирать данные на дисках, изменять названия и другие атрибуты файлов и так далее). Лечение от резидентных вирусов затруднено, так как даже после удаления зараженных файлов с дисков вирус

остается в оперативной памяти и возможно повторное заражение файлов.

Макровирусы являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и так далее). Для своего размножения такие вирусы используют возможности макроязыков и с их помощью переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макровирусы для Microsoft Office, использующие возможности языка Visual Basic for Applications.

При работе с документом пользователь выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и так далее. При этом приложение ищет и выполняет соответствующие *стандартные макросы*. Макровирусы содержат стандартные макросы, вызываются вместо них и заражают каждый открываемый или сохраняемый документ. Вредные действия макровирусов реализуются с помощью встроенных макросов (вставки текстов, запрета выполнения команд меню приложения и так далее).

Макровирусы являются *ограниченно резидентными,* то есть они находятся в оперативной памяти и заражают документы до тех пор, пока открыто приложение. Кроме этого, макро-вирусы заражают шаблоны документов и поэтому активизируются уже при запуске зараженного приложения.

Сетевые вирусы для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей. Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

Одним из наиболее эффективных способов борьбы с вредоносными программами является использование антивирусного программного обеспечения.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления вредоносных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту, поскольку на

любой алгоритм антивируса можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При использовании антивирусных программ необходимо иметь представление об особенностях их работы.

«Ложное срабатывание» – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

«Пропуск вируса» – недетектирование вируса в зараженном объекте.

«Сканирование по запросу» – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

«Сканирование на лету» – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и др.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Для защиты от вирусов и лечения зараженного компьютера используются антивирусные программы, которые по принципу действия можно разделить на *блокировщики, ревизоры* и *полифаги.*

Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. Например, «вирусоопасной» является запись в загрузочные сектора дисков, которую можно запретить с помощью программы BIOS Setup.

Ревизоры. Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов. Эти суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) сохраняются в базе данных антивируса. При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Полифаги. Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных

и новых (неизвестных полифагу) вирусов. Для поиска известных вирусов используются маски вирусов (некоторая постоянная последовательность программного кода, специфичная для каждого конкретного вируса).

Во многих полифагах используются также алгоритмы эвристического сканирования, то есть анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения (возможно, заражен или не заражен) для каждого проверяемого объекта.

Полифаги-мониторы постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени. Полифаги-сканеры производят проверку системы по команде пользователя.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Задание 1.

Разобрать инцидент в сфере кибербезопасности, установить степень вины каждого из участников события.

В NHS (National Hospital System, UK; Национальная система здравоохранения Объединённого Королевства) события развивались следующим образом. Исполнительный директор «МУРЕНА» поручил руководителю департамента информационных технологий «СИРЕНЕВЫЙ» установить обновления операционных систем на компьютерах работников Центрального офиса в срок до 20 июня в связи с сообщениями об обнаружении критической уязвимости в установленном программном обеспечении. Руководителю департамента HR «ФИОЛЕТОВЫЙ» было поручено ознакомить всех подчинённых с вновь вводимой политикой информационной безопасности в срок до 6 июня. В данной политике были описаны правила безопасного использования съемных носителей и электронной почты. 11 июня у менеджера по закупке «ЖЕЛТЫЙ» был первый рабочий день после отпуска. Ему позвонил руководитель отдела снабжения «СЕРЫЙ» и попросил срочно проверить и согласовать акты по объемам поставок медицинского инвентаря, предоставленные поставщиком. После проверки выяснилось, что представленные акты требуют корректировки. Новые акты подрядчик смог бы привезти только на следующий день, а руководитель просил разобраться с этой задачей как можно скорей. Представитель поставщика «ГОЛУБОЙ» предложил сразу внести корректировки и распечатать новый документ – у него была с собой печать организации. Исходный документ находился на рабочей флешке подрядчика. Менеджер по закупке вставил эту флешку в свой рабочий компьютер, проверил антивирусом и скопировал нужный файл. Затем они быстро внесли правки и уже заканчивали печатать акт, как на весь экран компьютера открылось окно с требованием заплатить выкуп в 300 долларов. В против-

ном случае все данные обещали безвозвратно уничтожить через пять дней. Менеджер попробовал перезагрузить компьютер, но это не помогло. После звонка в техподдержку ему стало известно, что сейчас то же самое происходит по всей сети NHS. Врачи начали один за другим жаловаться на невозможность открыть истории болезней пациентов. Результат инцидента – множество зараженных рабочих станций, зашифрованые файлы баз данных историй болезней пациентов. Как следствие – невозможность оказывать медицинские услуги населению.

На флешке поставщика оказался вирус, а на компьютер менеджера по закупке важные обновления для Windows не были установлены. Так же эти обновления еще не установили на некоторые другие компьютеры (длительное время не перезагружались сотрудниками). Комиссию по расследованию возглавляет руководитель департамента информационной безопасности «КРАСНЫЙ» .

Задание 2.

Гражданин А. 4.08.2022 выставил объявление на сайте Avito о продаже формы ППС. Через два дня по указанному на сайте им номеру с ним связались и сказали, что не получается оформить заказ, попросили перейти по ссылке для удобства дальнейшего общения и покупки товара. Дайте характеристику действиям покупателя.

Задание 3.

Разработчик потратил пять лет на создание приложения для смартфона. Когда приложение вышло в прокат, у мальчика возникло желание его приобрести, но узнав о высокой стоимости, решил обратиться в Интернет за помощью. В сети, перейдя по первой ссылке, мальчик увидел вторую ссылку, по которой данное приложение можно было скачать бесплатно. Из представленных ниже вариантов выберите тот, который Вы предложили бы мальчику, и аргументируйте свой ответ.

- Скачать игру с данного сайта, так как там она бесплатная.
- Купить в магазине.
- Продолжить искать игру в интернете с возможностью купить её со скидкой.

Задание 4.

Вам пришло письмо на электронную почту следующего содержания: «Для подтверждения того, что Вы являетесь настоящим пользователем «Вконтакте», перейдите по ссылке https://vvk.com/id47073790». Стоит ли переходить по ссылке и почему? Обоснуйте свой ответ.

Задание 5.

Подключившись к одной из обнаруженных открытых сетей «FreeWiFi» в торговом центре и зайдя на сайт интернет-магазина, девочка нашла необходимый ей товар и оформила онлайн-покупку, введя номер банковской карты и трехзначный код с обратной стороны карты.

1. Какие ошибки совершила Таня?
2. Какие негативные последствия совершенного ею поступка могут возникнуть? Обоснуйте свой ответ.
3. Сформулируйте правила, которыми нужно руководствоваться при использовании общественной Wi-Fi сети.

Задание 6.

Задание по подготовке доклада мальчик решил выполнить с помощью поиска готовых вариантов в Интернете. В поисковой строке он ввел тему доклада и перешел по первой же появившейся ссылке. Увидев в окне браузера яркую кнопку «скачать», нажал на нее. Неожиданно компьютер начал перезагрузку, а когда включился, то на рабочем столе исчезли все ярлыки. Что произошло с компьютером? Какие действия необходимо предпринять для выхода из создавшейся ситуации?

Задание 7.

Каким образом вирус может попасть в компьютер?

1) прослушивание музыки в социальных сетях (да/нет);
2) скачивание файлов со сторонних сайтов (да/нет);
3) работа в программах Microsoft Office (да/нет);
4) переход по подозрительным ссылкам из сообщений от неизвестных отправителей (да/нет);
5) просмотр фильмов, расположенных в памяти компьютера

(да/нет).

Сформулируйте правила, которыми нужно руководствоваться при работе в сети Интернет.

Задание 8.

На мобильный телефон Маши пришло СМС-сообщение от неизвестного отправителя: «Доброго времени суток! По вашим паспортным данным найдены страховые начисления в размере 200 руб. Подробности на сайте: http://snils-gost.online». Не задумываясь о последствиях, Маша перешла по ссылке. В открывшемся окне браузера не было никакой информации о паспортных данных, и Маша его закрыла. Через пару минут на мобильный телефон пришло СМС-сообщение от сотового оператора: «Ваш баланс менее 5 рублей». Связано ли исчезновение средств с переходом по ссылке из СМС-сообщения? Какие ошибки допустила Маша? Какие последствия могут возникнуть в результате действий Маши? Аргументируйте свой ответ. Составьте рекомендацию, в которой будет содержаться описание признаков СМС-мошенничества и правил поведения при встрече с ними.

Задание 9.

Соотнесите используемые средства защиты с их функциями:

1) DAM-решение	А) проверка соответствия данных национальным и международным стандартам
2) DCAP-система	Б) слежение за файлами, анализ содержимого файлов и присвоение им меток
3) SIEM-система	В) контроль и удержание важной информации
4) DLP-система	Г) являются базой для функционирования всех программ
5) Система контроля целостности	Д) анализ аномальной активности приложений
6) Шифрование	Е) контроль запросов к базам данных
7) IDS/IPS/EPS	Ж) контроль состояния IT-системы
8) NGFW	З) предохранение от вредоносных программ

9) Средства администрирования	И) слежение за целостностью и сохранностью информации

Задание 10.

Николаев искал в интернете, где можно купить одежду дешевле, чем в магазине. В интернет-магазине с низкими ценами он выбрал себе товары, положил в корзину и собирался оплатить. На сайте отсутствовала форма оплаты наложенным платежом или наличными курьеру, а при вводе карты был иностранный сервис с восточным языком. Стоит ли вводить данные своей платёжной карты, обоснуйте свой ответ.

Задание 11.

Вы заказали в интернет-магазине «оригинальные» кроссовки дорогого бренда. Оплата осуществлялась переводом денег (в размере 10 тысяч рублей) на Qiwi-кошелек продавца. Через сутки, почитав отзывы в интернете о продавце и осознав, что были обмануты, вы заполнили соответствующую заявку на сайте платежной системы Qiwi о том, что перевели деньги мошеннику. При этом создали и сохранили скриншоты переписки. Какие у вас шансы вернуть деньги?

Задание 12.

Вам сообщили, что некто обращается к друзьям и знакомым в социальной сети, собирая о Вас информацию с целью поиска компрометирующих данных. Что будет этому некто? Как поступить Вам в данной ситуации?

Задание 13.

Егоров И.И. с июля по октябрь 2020 г. совершил серию краж с банковского счета. Потерпевшие лишались денежных средств, принимая участие в акции, якобы организованной банком. Условия её были просты: необходимо заполнить анкету, для того чтобы на счёт поступили бонусы в виде денежных средств. Жертвы мошенника указывали в анкете реквизиты своих банковских карт. Через некоторое время с их счетов списывались деньги. Молодым

человеком похищены денежные средства на общую сумму порядка 50 тысяч рублей. Какие ошибки в сфере кибербезопасности совершили личности, участвующие в данной акции? Как можно защититься от подобного рода мошенничеств?

Задание 14.

Вы получили СМС- или ММС-сообщение со ссылкой на скачивание музыки, картинки или программы. Перейдёте ли вы по указанной ссылке? Ответ обоснуйте.

Задание 15.

Вы решили приобрести телефон по цене, которая ниже рыночной, но продавец просит перечислить предоплату на сайте магазина и отправляет ссылку для неё. Перейдете ли Вы по данной ссылке и стоит ли доверять магазинам, работающим со сторонними способами оплаты?

Задание 16.

Вы ищете подрядчиков для строительства частного дома на своём участке. Найдя исполнителя через сервис соискателей AVITO, обговорили все детали, составили смету и договорились о времени встречи, после этого Вас просят перечислить предоплату в качестве задатка, для того чтобы “зря не дёргать бригаду”. Стоит ли соглашаться на подобного рода условия при том, что подрядчик предложил очень низкую стоимость работ.

Задание 17.

Иван Ю.Ю. нашел для себя новое хобби в виде развлекательной онлайн-игры, в которой решающим фактором силы является игровой опыт. Иван нашёл игрока, который согласился продать игровую валюту за реальные деньги, но просит деньги вперёд. Стоит ли соглашаться на подобного рода условия? Как можно вернуть деньги в случае мошенничества?

Задание 18.

Вам звонит неизвестный номер и предлагает взять кредит под процентную ставку 1% годовых. Вы согласились и продиктовали

свои паспортные данные, правильно ли вы поступили? Какие возможные последствия будут иметь такие действия?

Задание 19.

Гражданин М. получил на телефон сообщение, в котором говорилось о том, что его близкий родственник попал в серьёзное ДТП, вследствие чего требуется перевести 56 тысяч рублей по следующему номеру: +79872736723. Должен ли гражданин М. перечислять денежные средства? Как в конечном счёте необходимо реагировать на подобного рода сообщения?

Задание 20.

Гражданке Л. на электронную почту от хорошо известного ей человека без предупреждения пришло письмо с файлом большого объема, имеющее расширение exe. Стоит ли открывать данное письмо? Если нет, то объясните почему.

ТЕСТОВЫЕ ВОПРОСЫ

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- разработка аппаратных средств обеспечения правовых данных;
- разработка и установка во всех компьютерных правовых сетях журналов учета действий;
- разработка и конкретизация правовых нормативных актов обеспечения безопасности.

2. Заключительным этапом построения системы защиты является:

- сопровождение;
- планирование;
- анализ уязвимых мест.

3. Все средства связи, используемые во взаимоувязанной сети связи Российской Федерации, подлежат обязательной сертификации на соответствие установленным стандартам, иным нормам и техническим требованиям.

- да;
- нет;
- только объекты правительственной связи.

4. Основными источниками угроз информационной безопасности являются:

- хищение жестких дисков, подключение к сети, инсайдерство.
- перехват данных, хищение данных, изменение архитектуры системы.
- хищение данных, подкуп системных администраторов, нарушение регламента работы.

5. Наиболее важным при реализации защитных мер политики безопасности является:

- аудит, анализ затрат на проведение защитных мер.
- аудит, анализ безопасности.
- аудит, анализ уязвимостей, риск-ситуаций.

6. ... – это степень защищенности информации от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного использования.

- уязвимость информации
- защищенность информации
- надежность информации
- безопасность информации

7. Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний;
- органы права, государства, бизнеса;
- сетевые базы данных, фаерволлы.

8. Под информационной безопасностью понимается:

- защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;
- программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;
- нет верного ответа.

9. Шифрование – это …

- способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого;
- совокупность тем или иным способом структурированных данных и комплекса аппаратно-программных средств;
- удобная среда для вычисления конечного пользователя.

10. Что такое план реагирования на инциденты кибербезопасности?

- совокупность документов, регулирующих порядок действий сотрудника при кибератаках;
- набор инструкций, которые помогут сотрудникам выявлять инциденты кибербезопасности, реагировать на них и восстанавливаться;
- действия по защите конфиденциальной информации.

11. Основными рисками информационной безопасности являются:

- искажение, уменьшение объема, перекодировка информации;
- техническое вмешательство, выведение из строя оборудования сети;
- потеря, искажение, утечка информации.

12. Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?

- аппаратный;
- программный;
- ручной;
- электромеханический.

13. Какие действия необходимо предпринимать в случае кибератаки?

- не запускать антивирусные программы и лечебные утилиты, не форматировать жесткий диск;
- выключить компьютер;
- перезапустить систему безопасности;
- включить антивирусные программы и лечебные утилиты.

14. Принципом политики информационной безопасности является принцип:

- невозможности миновать защитные средства сети (системы);
- усиления основного звена сети, системы;
- полного блокирования доступа при риск-ситуациях.

15. Укажите нормативный правовой акт, в котором раскрывается понятие «информационная безопасность».

- Закон Российской Федерации от 27.12.1991 № 1224-11 «О средствах массовой информации»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Доктрина информационной безопасности;
- все ответы верны.

16. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защитные КС;
- небезопасные КС;
- самодостаточные КС;
- саморегулирующиеся КС.

17. Информация, которую следует защищать (по нормативам, правилам сети, системы), называется:

- регламентированной;
- правовой;
- защищаемой.

18. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- длина шифрованного текста должна быть равной исходному тексту;
- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- нет правильного ответа.

19. Потенциальные угрозы, против которых направлены технические меры защиты?

- потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей;

- потери информации из-за халатности обслуживающего персонала и неведения системы наблюдения;
- потери информации из-за недостаточной установки резервных систем электропитания и оснащения помещений замками;
- процессы преобразования, из-за которых информация удаляется.

20. Какие угрозы безопасности информации являются преднамеренными:
- ошибки персонала;
- открытие электронного письма, содержащего вирус;
- неавторизованный доступ.

21. Один из самых известных методов шифрования носит имя…
- Цезаря;
- Гейца;
- Вижинера.

22. Что включает план реагирования на инциденты кибербезопасности?
- меры, выявляющие угрозы информационной безопасности;
- меры, предотвращающие угрозы информационной безопасности;
- меры, которым следует следовать, чтобы предотвратить кибер-атаки, шаги, которые необходимо предпринять, когда компания с атакой уже столкнулась, а также меры после атаки.

23. Средством предотвращения потерь информации при кратковременном отключении электроэнергии является …
- источник бесперебойного питания (UPS);
- источник питания;
- электропереключатель;
- все перечисленное.

24. Способ защиты информации от сбоев устройств для хранения информации?

- установка систем бесперебойного питания (UPS);
- симметричное мультипроцессирование;
- периодическое сохранение данных;
- организация надежной системы резервного копирования и дублирования данных

25. Элемент аппаратной защиты, где используется экранирование, фильтрация, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений?

- защита от сбоев в электропитании;
- защита от сбоев серверов, рабочих станций, локальных компьютеров;
- защита от сбоев устройств для хранения информации;
- защита от утечек информации электромагнитных излучений.

26. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности;
- регламент информационной безопасности;
- политическая информационная безопасность;
- протекторат.

27. Какие действия необходимо предпринимать в случае кибератаки?

- не запускать антивирусные программы и лечебные утилиты, не форматировать жесткий диск;
- выключить компьютер;
- перезапустить систему безопасности;
- включить антивирусные программы и лечебные утилиты.

28. Основная масса угроз информационной безопасности приходится на:

- троянские программы;

- шпионские программы;
- черви.

29. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

- программные, технические, организационные, технологические;
- серверные, клиентские, спутниковые, наземные;
- личные, корпоративные, социальные, национальные.

30. Процессы, методы поиска, сбора, хранения, обработки предоставления и распространения информации, способы осуществления таких процессов и методов – это …

- информационные технологии;
-информационная система;
-информационно-телекоммуникационная сеть.

31. Цели кибербезопасности – своевременное обнаружение, предупреждение ...

- атаки аппаратных средств обеспечения правовых данных;
- несанкционированного доступа и воздействия на информацию в сети;
- инсайдерских атак на информационные системы организации;
- чрезвычайных ситуаций в сфере информационной безопасности.

32. Основные объекты кибербезопасности – это ...

- государственные органы, юридические лица и бизнес-организации;
- компьютерные сети, базы данных, электронные носители информации;
- информационные системы и психологическое состояние пользователей;
- бизнес-ориентированные, коммерческие, экспертные системы.

33. Основными субъектами кибербезопасности являются:

- компьютерные сети, базы данных государственных органов;

- государственные органы, юридические лица и бизнес-организации;
- сетевые базы данных, фаерволлы юридических лиц и бизнес-организаций;
- программное обеспечение государственных органов, юридических лиц и бизнес-организаций.

34. Принципом политики кибербезопасности является принцип:

- невозможности незаметно миновать защитные средства сети (системы);
- усиления и обеспечения безопасности основного звена сети, системы;
- перехода в безопасное состояние работы сети, системы;
- полного блокирования доступа при риск-ситуациях.

35. Принципом политики кибербезопасности является принцип:

- одноуровневой защиты сети, системы;
- усиления защищенности самого незащищенного звена сети (системы);
- перехода в безопасное состояние работы сети, системы;
- полного доступа пользователей ко всем ресурсам сети, системы.

36. Принципом политики кибербезопасности является принцип:

- распределения и контроля доступа пользователей;
- одноуровневой защиты сети, системы;
- совместимых, однотипных программно-технических средств сети, системы;
- точечного регулирования уязвимостей.

37. ЭП, как средство идентификации и верификации пользователей, – это:

- электронный преобразователь;
- электронная подпись;

- электронный процессор;
- электронная площадка.

38. Наиболее распространенными средствами воздействия на сеть являются:

- снижение трафика, информационный обман, вирусы в сети Интернет;
- вирусы, логические мины (закладки), перехват сетевого трафика;
- компьютерные сбои, изменение системы администрирования и топологии сети;
- наводки, искажение информации, подмена оборудования.

39. Утечкой информации в системе называется ситуация, характеризуемая:

- утратой конфиденциальности;
- нарушением целостности;
- потерей доступности;
- искажением достоверности.

40. Как называется умышленно искаженная информация?

- дезинформация;
- информативный поток;
- достоверная информация.

41. Как называется информация, к которой ограничен доступ?

- конфиденциальная;
- противозаконная;
- открытая;
- недоступная.

42. Какими путями может быть получена информация?

- проведением, покупкой и противоправным добыванием информации научных исследований;
- захватом и взломом ПК информации научных исследований;

- добыванием информации из внешних источников и скремблированием информации научных исследований;
- захватом и взломом защитной системы для информации научных исследований.

43. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защитные КС;
- небезопасные КС;
- самодостаточные КС;
- саморегулирующиеся КС.

44. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности;
- регламент информационной безопасности;
- политическая информационная безопасность;
- протекторат.

45. Что называют защитой информации?

- все ответы верны;
- деятельность по предотвращению утечки защищаемой информации;
- деятельность по предотвращению несанкционированных воздействий на защищаемую информацию;
- деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию.

46. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- защита от сбоев в электропитании;
- защита от сбоев серверов, рабочих станций, локальных компьютеров;
- защита от сбоев устройств для хранения информации;
- защита от утечек информации электромагнитных излучений.

47. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем?

- защита от сбоев в электропитании;
- защита от сбоев серверов, рабочих станций, локальных компьютеров;
- защита от сбоев устройств для хранения информации;
- защита от утечек информации электромагнитных излучений.

48. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных – это ...

- защита от сбоев в электропитании;
- защита от сбоев серверов, рабочих станций, локальных компьютеров;
- защита от сбоев устройств для хранения информации;
- защита от утечек информации электромагнитных излучений.

49. Элемент аппаратной защиты, где используется экранирование, фильтрация, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений – это ...

- защита от сбоев в электропитании;
- защита от сбоев серверов, рабочих станций, локальных компьютеров;
- защита от сбоев устройств для хранения информации;
- защита от утечек информации электромагнитных излучений.

50. Какая из перечисленных атак на поток информации является пассивной?

- перехват;
- имитация;
- модификация;
- фальсификация;
- прерывание.

51. К открытым источникам информации относятся:

- газеты, радио, новости;

- информация, украденная у спецслужб;
- информация из вскрытого сейфа;
- информация, украденная из правительственной организации.

52. Какие технические каналы утечки отвечают за распространение звуковых колебаний в любом звукопроводящем материале или среде?

- акустические и виброакустические;
- электрические;
- оптические;
- радиоканалы.

53. Какие технические каналы отвечают за электромагнитные излучения радиодиапазона?

- акустические и виброакустические;
- электрические;
- оптические;
- радиоканалы.

54. Какие технические каналы утечки отвечают за напряжение и токи в различных токопроводящих коммуникациях?

- акустические и виброакустические;
- электрические;
- оптические;
- радиоканалы.

55. Какие технические каналы утечки отвечают за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- акустические и виброакустические;
- электрические;
- оптические;
- радиоканалы.

56. Технические каналы утечки информации делятся на:

- все перечисленное;

- акустические и виброакустические;
- электрические;
- оптические;
- радиоканалы.

57. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий – это ...

- индивидуальный подход к защите;
- комплексный подход к защите;
- смешанный подход к защите;
- рациональный подход к защите.

58. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия, задержек в доступе?

- информационная безопасность;
- защитные технологии;
- заземление;
- конфиденциальность.

59. Какие бывают потери информации, связанные с несанкционированным доступом?

- несанкционированное копирование, уничтожение, или подделка информации;
- потери при заражении систем компьютерными вирусами;
- случайное уничтожение или изменение данных;
- сбои дисковых систем.

60. Вид защиты баз данных?

- защита всех учетных записей, защита идентифицированных объектов;
- защита учетной записи группы администратора;
- защита приложения, которое используется для управления БД;
- защита группы USERS.

61. К наиболее важному элементу аппаратной защиты можно отнести ...

- защита от сбоев серверов, рабочих станция, и локальных компьютеров;
- защита от вирусов;
- защита от хакеров;
- все перечисленное.

62. Что такое инцидент кибербезопасности?

- любое событие, которое нарушает политику ИТ-безопасности организации и подвергает риску конфиденциальные данные;
- событие, подвергающее риску личную безопасность сотрудника;
- неприятный случай в политике конфиденциальности;
- мероприятие, направленное на защиту данных.

63. Назовите распространенные типы инцидентов:

- заражение вредоносным ПО, DDoS-атаки;
- атаки программ-вымогателей;
- внутренние атаки и фишинг;
- все вышеперечисленное.

64. Для чего нужен план реагирования на инциденты кибербезопасности?

- для предотвращения кибератак;
- для устранения случайных угроз;
- для защиты информации.

65. Укажите какие бывают виды инцидента по степени влияния?

- высокие и низкие;
- нет, низкое, среднее, высокое;
- такой классификации нет.

66. В течение какого времени должны разрешаться инциденты с высоким приоритетом?

- в течение 2-6 часов;

- в течение 24 часов;
- в течение первого часа;
- в течение месяца.

67. В течение какого времени должны разрешаться инциденты с низким приоритетом?

- в течение 1 года;
- в течение суток;
- в течение недели;
- в течение 2 часов.

68. Нужно ли обновлять план реагирования на инциденты кибербезопасности?

- да;
- нет.

69. Какое ПО позволяет продолжать бизнес-операции, даже если действия по реагированию на инциденты выполняются в фоновом режиме?

- антивирусное ПО;
- ПО для защиты конечных точек;
- ПО сетевой безопасности;
- все вышеперечисленное.

70. Значительная часть инцидентов являются … и нуждаются в базовом реагировании без участия специалистов кибербезопасности.

- критическими;
- типовыми;
- базовыми.

71. … требуют пристального внимания экспертов с момента обнаружения.

- критические инциденты;
- типовые инциденты;
- базовые инциденты.

72. Какие действия необходимо предпринимать в случае кибератаки?

- не запускать антивирусные программы и лечебные утилиты, не форматировать жесткий диск;
- выключить компьютер;
- перезапустить систему безопасности;
- включить антивирусные программы и лечебные утилиты.

73. Процесс анализа рисков при разработке системы защиты ИС включает:

- анализ потенциальных угроз, оценку возможных потерь;
- анализ системы безопасности;
- оценку результатов работы специалистов кибербезопасности.

74. Из перечисленных свойств безопасная система включает:

- доступность, целостность;
- конфиденциальность;
- все вышеперечисленное.

75. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:

- уровень безопасности;
- уровень защиты;
- степень угрозы;
- уровень угрозы.

76. С помощью закрытого ключа информация ...

- расшифровывается;
- зашифровывается.

77. При качественном подходе риск измеряется в терминах, ...

- заданных с помощью шкалы или ранжирования;
- установленных нормативами;
- утвержденных специалистами безопасности.

78. С использованием прикладных ресурсов ИС связан уровень ОС ...

- приложений;
- ПО;
- утилит;
- прикладных ПО.

79. Угрозы безопасности по природе происхождения квалифицируются как:

- преднамеренная/ случайная;
- сложная/ простая;
- квалифийцирующая/ обычная.

ЗАКЛЮЧЕНИЕ

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности. В связи с этим большое значение приобретает проблема культуры безопасного поведения в киберпространстве.

В настоящем пособии были наглядно рассмотрены основные вопросы, связанные с понятием и обеспечением информационной и кибербезопасности в органах внутренних дел Российской Федерации. Знание и соблюдение основ информационной безопасности и защиты информации существенно повысит уровень защищенности информации ограниченного доступа и распространения, сопровождающей деятельность органов внутренних дел Российской Федерации.

Использование полученных знаний, умений и навыков в профессиональной служебной деятельности субъектов информационных отношений органов внутренних дел Российской Федерации позволит соблюдать необходимые требования по работе с информацией ограниченного распространения и доступа в рамках информационных систем и ведомственных информационных ресурсов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 30.12.2008 № 6-ФКЗ и № 8-ФКЗ) // СПС «Консультант плюс». URL: http://www.consultant.ru/

2. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 06.02.2020) 646 // СПС «Консультант плюс». URL: http://www.consultant.ru/

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.12.2019) (с изм. и доп., вступ. в силу с 13.12.2019) // СПС «Консультант плюс». URL: http://www.consultant.ru/

4. О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ (в ред. от 06.02.2020) // СПС «Консультант плюс». URL: http://www.consultant.ru/

5. О государственной тайне: закон Российской Федерации от 21.07.1993 № 5485-1 (в ред. от 29.07.2018) // СПС «Консультант плюс». URL: http://www.consultant.ru/

6. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 06.06.2019, с изм. и доп., вступ. в силу с 01.11.2019)// СПС «Консультант плюс». URL: http://www.consultant.ru/

7. Доктрина информационной безопасности Российской Федерации: утверждена указом Президента Российской Федерации 05.12.2016 № 646 // СПС «Консультант плюс». URL: http://www.consultant.ru/

8. План мероприятий по направлению Информационная безопасность программы Цифровая экономика Российской Федерации: приложение № 4 к протоколу заседания Прави-

тельственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 18.12.2017 № 2. URL: http://static.government.ru/

9. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. URL: http://kremlin.ru/acts/news/55146

10. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26.07.2017 № 193-ФЗ. URL: http:// www.consultant.ru/

11. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26.07.2017 № 194-ФЗ. URL: http://kremlin.ru/acts/news/55148

12. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. Приказов ФСТЕК России от 09.08.2018 № 138, от 26.03.2019 № 60, от 20.02.2020 № 35). URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

13. Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: № 149/2/7-200 от 24.12.2016. URL: https://secret-net.ru/services/zashchita-informatsii

Основная литература:

1. Внуков А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2021. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8.

2. Внуков А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А.А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2021. – 161 с. – (Профессиональное образование). – ISBN 978-5-534-13948-8.

3. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. – Москва : Издательство Юрайт, 2021. – 104 с. – (Высшее образование). – ISBN 978-5-534-14590-8.

4. Суворова Г.М. Информационная безопасность: учебное пособие для вузов / Г.М. Суворова. – Москва : Издательство Юрайт, 2021. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0.

5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией А.А. Стрельцова. – Москва : Издательство Юрайт, 2021. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8.

Дополнительная литература:

1. Щеглов А.Ю. Защита информации: основы теории: учебник для вузов / А.Ю. Щеглов, К.А. Щеглов. – Москва : Издательство Юрайт, 2021. – 309 с. – (Высшее образование). – ISBN 978-5-534-04732-5.

2. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А.И. Белоус, В.А. Солодуха // Издательство: Москва: Техносфера. – 2021. – 483 с. ISBN: 978-5-94836-612-8.

3. Диогенес Ю. Кибербезопасность. Стратегии атак и обороны / Ю. Диогенес, Э. Озкайя // Издательство: ДМК Пресс. – 2020. – 326 с. ISBN: 978-5-97060-709-1.

4. Белоус А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А.И. Белоус, В.А. Солодуха // Издательство: Инфра-Инженерия. – 2020. – 692 с. ISBN: 978-5-9729-0486-0.

5. Александрова Е.Б. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Е.Б. Александрова, Д.П. Зегжда, М.О. Калинин и др. // Издатель-

ство: Горячая Линия – Телеком. – 2020. – 560 с. ISBN: 978-5-9912-0827-7-25.

6. Пол Тронкон. Bash и кибербезопасность. Атака, защита и анализ из командной строки / Пол Тронкон, Карл Олбинг // Издательство: Питер – 2020. – 288 стр. ISBN: 978-5-4461-1514-3

7. Основы информационной безопасности: учебник : рек. УМО в обл. национальной безопасности / В.Ю. Рогозин и др. Москва: ЮНИТИ-ДАНА, 2017. – 287 с.

8. Каримов А.М. Информатика и информационные технологии в профессиональной деятельности: учебное пособие / А.М. Каримов, Г.Д. Марданов, С.В. Смирнов. – Казань: КЮИ МВД России – 120 с., 2020.

Учебное издание

Каримов Адель Миннурович
Смирнов Сергей Викторович
Марданов Георгий Дамирович

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебно-практическое пособие

Корректура, компьютерная верстка
О.В. Добрыдневой

Подписано в печать
Формат 60х84 1/16 Усл. печ. л. 4 Тираж 60 экз.

Типография КЮИ МВД России
420059, г. Казань, ул. Оренбургский тракт, 130