ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИИ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Каримов Х.Т.[1], Пермяков В.Н.[2], Тархова Л.М.[3], Урманов В.Г.[4], Юзмухаметов К.З.[5], Ямилев И.Р.[6], Гусев Д.А.[7], Талыпов М.А.[8], Багаутдинова И.И.[9], Дик Е.Н.[10]

Ключевые слова: *информационная безопасность, коммуникационные технологии, локальные и глобальные сети, биометрический контроль, кибербезопасность, безопасность сетей, взлом.*

Аннотация

Цель исследования: изучение проблем информационной безопасности в органах внутренних дел России. С бурным развитием информационно-коммуникационных технологий происходит и развитие угроз, возникающих при недостаточном соблюдении элементарных правил пользования этими технологиями. В статье рассмотрены подобные проблемы не только обычных пользователей, но и сотрудников органов внутренних дел.

Методы исследования: предлагаются пути решений возникающих проблем. Актуальность данной темы обусловлена ростом преступлений в области информации: кража, взлом, уничтожение, порча, что требует улучшения механизмов защиты от этих угроз. Описаны теоретические аспекты информационной безопасности в локальной и глобальной сети. Использованы методы сравнения. Подробно описана процедура использования анонимного биометрического контроля доступа.

Полученные результаты: предложены решения проблем информационной безопасности как простых пользователей, так и сотрудников органов внутренних дел России. Как одно из решений ряда проблем информационной безопасности предлагается сформировать системный подход к данной проблеме. Необходимо улучшать комплексные средства защиты.

DOI: 10.21681/1994-1404-2024-2-170-180

[1] ***Каримов Хасан Талхиевич,*** *кандидат технических наук, доцент кафедры управления в органах внутренних дел, Уфимский юридический институт МВД России, г. Уфа, Российская Федерация. ORCID: 0000-0003-1837-7052, ResearcherID: RIDG-5422-2018.*
E-mail: krig.blits@mail.ru

[2] ***Пермяков Валерий Николаевич,*** *кандидат технических наук, доцент кафедры прикладной механики и компьютерного инжиниринга, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: ir.perm@yandex.ru

[3] ***Тархова Ляйля Мукаддасовна,*** *кандидат технических наук, доцент, доцент кафедры прикладной механики и компьютерного инжиниринга, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: tarkhova@inbox.ru

[4] ***Урманов Виль Губаевич,*** *кандидат технических наук, доцент кафедры прикладной механики и компьютерного инжиниринга, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: uvg55@mail.ru

[5] ***Юзмухаметов Кирилл Зинурович,*** *курсант 4 курса факультета подготовки следователей, Уфимский юридический институт МВД России, г. Уфа, Российская Федерация.*
E-mail: mr.kiryt@mail.ru

[6] ***Ямилев Инсаф Римович,*** *аспирант, Уфимский университет науки и технологий, г. Уфа, Российская Федерация.*
E-mail: yuristyamilev@gmail.com

[7] ***Гусев Дмитрий Александрович,*** *кандидат технических наук, доцент, доцент кафедры прикладной механики и компьютерного инжиниринга, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: bsau-ngg@yandex.ru

[8] ***Талыпов Марат Артурович,*** *кандидат биологических наук, старший преподаватель кафедры землеустройства, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: talypovmarat@yandex.ru

[9] ***Багаутдинова Ильнара Илфировна,*** *кандидат технических наук, старший преподаватель кафедры прикладной механики и компьютерного инжиниринга, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: isalimyanova@mail.ru

[10] ***Дик Елизавета Николаевна,*** *кандидат психологических наук, доцент кафедры математики, Башкирский государственный аграрный университет, г. Уфа, Российская Федерация.*
E-mail: lizadik@mail.ru

Введение

С непрерывным развитием сетевых технологий производство и образ жизни людей также заметно меняются. Люди считают, что сеть делает доступ к информации быстрее и удобнее, но это также делает использование сети более прозрачным и открытым. Совместное использование и удобство сети облегчают нарушителям посягательства на права других лиц, а именно, на неприкосновенность частной жизни, оказывая беспрецедентное влияние на традиционную защиту информации. Актуальность данной работы обусловлена возрастающей информационной опасностью как для частных лиц, так и для сотрудников органов внутренних дел, что наталкивает на поиск решений против нарастающей проблемы. В этой научной работе изучаются алгоритмы, связанные с обеспечением информационной безопасности в жизни людей и в органах внутренних дел; её задача — построить модель обеспечения информационной безопасности. Целью является анализ, в рамках этой модели, некоторых событий нарушения конфиденциальности, существующих сегодня в сети знаний и взглядов на закон. Вопрос о том, как успешно решать проблемы информационной безопасности, имеет большое практическое значение для многих стран; чем более распространенными или опасными становятся проблемы информационной безопасности, тем важнее иметь эффективные гарантии безопасности. Информационные технологии непрерывно развиваются, и это приводит к тому, что информационная безопасность становится одним из главных аспектов изучения для многих умов. Фактор безопасности различных классов системы обработки информации играет главную роль. Различные способы, например, анонимный биометрический контроль доступа, помогут защитить информацию в органах внутренних дел от несанкционированного завладения и доступа.

Методология (материалы и методы)

Информационная безопасность — защищенность системы от всех воздействий, которые направлены на её разрушение и попытки хищения информации.

Разрушение информационных ресурсов происходит под процессом деформирования информации ресурсов или программного аппаратного обеспечения.

Угрозы безопасности подразделяются на случайные и преднамеренные. Они носят существенный характер и серьезный ущерб. В этой работе раскрываются умышленные угрозы, которые отличаются от случайных тем, что имеют цель нанесения ущерба пользователю Интернета.

Взломщик, мошенник, хакер — довольно много терминов присущи человеку, цель которого деформировать работу информационных систем, получить информацию, которая защищена и не доступна в открытых источниках информации. Их задача — найти источники конфиденциальной информации, в котором можно легко обойти защиту и получить доступ к информации.

Источник информации — материальный объект, имеющий сведения и данные, которые злоумышленники могут использовать для получения выгоды или разрушения системы. В настоящее время необходимо проанализировать комплексный подход с применением взаимосвязанных мер защиты. В нынешнее время можно утверждать о новой современной инновационной технологии защиты информации в Интернете и в информационных компьютерных системах.

В современности преступники используют сеть Интернет для завладения информацией и денежными средствами пользователей и сотрудников органов внутренних дел. Масштабы проблемы большие, следовательно, требуют самой активной работы по усовершенствованию защиты информации от хакеров. В России компьютерная преступность вызывает большой резонанс, так как кибератаки ведутся и за рубежом в результате умелых махинаций, проводимых хакерами, иностранные банки теряют большие суммы денег.

Вот для примера данные из других стран за 2 квартал 2023 года: 87% организаций в Великобритании в разные промежутки времени попадали под угрозу интернет-преступников, 20% фирм стали жертвами в Нидерландах. С помощью кибертехнологий в Германии похищается 6 млрд евро. Эксперты также отмечают высокий уровень латентных преступлений такого рода: 90,9% случаев компьютерного пиратства не раскрываются [1, 2].

Киберпреступность стала разрушающим фактором экономики государств. Ухудшается положение тем, что правоохранительные органы также плохо защищены от угрозы атак со стороны преступников. Именно сейчас очень актуальна проблема защиты собственной информации в органах внутренних дел. Это самая важная задача на фоне развития всемирной сети Интернет и информационных систем.

Информационная безопасность органов внутренних дел России

В современном мире, построенном на широком использовании компьютерных технологий, подход к пониманию информации полностью изменился. С появлением компьютеров информация стала восприниматься как одна из неотъемлемых составляющих жизни любого человека. Наряду с этим взгляд на информацию изменился с восторженного на обыденный [3, 4].

Что такое информация? Почему она нуждается в обработке и, более того, в правовой защите?

Подразделить информацию можно на правовую и неправовую; правовая также делится на нормативную и ненормативную.

Нормативная содержится в нормативных правовых актах и создается в последовательности законотворческой деятельности. Сюда можно отнести Конституцию Российской Федерации, федеральные конституцион-

ные законы, федеральные законы, законодательные акты субъектов Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации, другие акты органов исполнительной власти всех уровней нормативного характера, а также акты органов местного самоуправления. Ненормативная правовая информация образуется на разных этапах работы в правоохранительной и правоприменительной деятельности, она содержится в процессуальных документах [5].

В соответствии с ней исполняются предписания нормативных правовых актов. Такую информацию можно разделить на группы:

1. Информация о состоянии правопорядка.

2. Информация о гражданско-правовых отношениях, договорных и иных обязательствах (контрактах, соглашениях и т. д.).

3. Информация, представляющая административную деятельность органов исполнительной власти и местного самоуправления по исполнению нормативных предписаний.

4. Информация о судах и судебных органах (судебные дела и судебные решения).

5. Информация правоохранительного характера.

Элементами информационной системы органов внутренних дел России являются:

1) ведомственные информационные и информационные ресурсы, ИСОД;

2) ведомственная информационная инфраструктура — инструменты и системы информатизации;

3) субъекты информационной деятельности — сотрудники внутренних органов;

4) система регулирования.

Информационная безопасность в области обороны и правосудия [6, 7]:

1) ресурсы федеральных органов исполнительной власти, выполняющих функции правоохранительных органов, органов судебной власти, их информационно-вычислительных центров, содержащие оперативную информацию и данные;

2) центры обработки данных и техническая, программная и нормативная поддержка;

3) информационная инфраструктура.

В марте 2012 года МВД России утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России в 2012—2014 гг. Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства [8, 9].

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, который велся с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и государственными органами различных уровней.

ИСОД является помощником для органов внутренних дел. Информационно-аналитическое обеспечение деятельности для оперативных сотрудников, участковых и следователей является важной частью работы с информацией. Данные, которые содержатся в ИСОД, являются особо важной оперативной информацией, как и учеты органов внутренних дел, особенно дела оперативного учета.

У каждого сотрудника имеется свой компьютер с доступом в ИСОД, они соединяются через локальную сеть; посредством доступа к нему можно получить различные оперативно важные данные [10, 11]. Нельзя допускать физический и любой несанкционированный доступ к таким компьютерам. Информация, которая там содержится, находится под особой охраной, и ее утечка может нанести серьезный ущерб сотрудникам и всей системе правоохранительных органов. Ниже разберем основные угрозы для безопасности такой информации [12, 13].

Доступ к информации имеют только действующие сотрудники, но при увольнении может произойти непоправимое: существующая проблема «несогласия» сотрудника с решением руководства может натолкнуть на продажу или использование данных для своей выгоды. Сотрудникам службы собственной безопасности МВД России (в их компетенцию входит проведение опросов и тестов у сотрудников на выявление фактов нарушения законодательства или укрывательства других противоправных действий их коллег), морально-психологическому отделению органов внутренних дел необходимо проводить психологическое тестирование на предмет выявления конфликтных ситуаций в подразделениях и угрозы со стороны сотрудников. Такие тестирования должны быть строго конфиденциальными, что поможет определить проблемы в коллективе для дальнейших их решений [14].

Реальные внутренние и внешние угрозы опасны как в судебной системе, так и в правоохранительных органах [15, 16].

В числе внешних информационных угроз:

– разведывательная деятельность спецслужб иностранных государств, международных преступных организаций, организаций и групп по сбору сведений о раскрытии задач, планов деятельности, методов работы и мест дислокации специальных подразделений и внутренних органов;
– деятельность иностранных государственных и частных хозяйствующих субъектов, пытающихся получить несанкционированный доступ.

Внутренними угрозами являются:

– несоблюдение установленных правил сбора, обработки, хранения и передачи информации, хранящейся в автоматизированных архивах и базах данных, используемых для расследования преступлений;

– отсутствие правового и нормативного регулирования обмена информацией в правоохранительной и судебной сферах;
– отсутствие целостной методологии сбора, обработки и хранения судебной, статистической и оперативной информации.

Выразить безопасность информационных ресурсов и информационной структуры возможно через безопасность их наиболее важных свойств.

Информационные ресурсы и инфраструктуры органов внутренних дел можно защитить через безопасность их важных свойств. Субъектам пользователей может причинить ущерб воздействие на критические важные средства обработки информации и процессы.

Каждый компонент автоматизированной системы (АС) нуждается в безопасности [17], и она формируется из обеспечения трех его характеристик:
– конфиденциальность, которая заключается в том, что информация доступна только уполномоченным субъектам;
– целостность, т. е. умение информации противостоять несанкционированному воздействию, истреблению или искажению;
– доступность, которая выражается в том, что при наличии полномочий доступ к необходимому компоненту системы возможен в любой момент без особых проблем.

Если такие характеристики нарушаются, то это создает непосредственную угрозу информационной безопасности органов внутренних дел [18, 19].

Информация, которая находится в АС, нуждается в защите от разглашения, искажения, потери или незаконного тиражирования ее, а также минимизации причиненного ущерба, если такой есть.

Угрозы информационной безопасности

В.А. Галатенко [20] выделяет несколько основных механизмов безопасности:
– управление доступом,
– идентификация и аутентификация,
– протоколирование и аудит,
– криптография и экранирование,

для эффективного использования которых необходимо применить опережающий анализ предполагаемых угроз.

Для обеспечения информационной безопасности необходимо строго распределить функции пользователей, администраторов серверов и локальных сетей и руководства органов внутренних дел.

В то же время должна быть разработана стратегия распределения обязанностей и функций между сотрудниками органов внутренних дел.

Об изменении статуса сотрудника должны знать все остальные работники; руководство также информирует личный состав об утверждении положении политики безопасности.

Причины увольнения сотрудника могут быть различными, но он может быть не согласен с решением руководства. В этом случае уволенный сотрудник может представлять опасность для отдела или подразделения, в котором работал.

При несогласии сотрудника с решением об увольнении он, имея информацию об основных принципах функционирования системы, может прибегнуть к попытке изменения, удаления или распространения служебной информации. После увольнения сотрудника права на доступ к информационным ресурсам необходимо незамедлительно аннулировать.

Основная проблема соотношения средств и целей не должна стоять на втором плане: затраты на меры защиты должны сопоставляться со стоимостью ущерба, который может причинить злоумышленник [21].

Обеспечивать бесперебойное функционирование сети, применять меры по безопасности и следить за выполнением политики безопасности должны администраторы локальных сетей. Они несут ответственность за безопасность серверов и следят за тем, чтобы механизмы конфиденциальности информации соответствовали общим принципам политики безопасности.

Простой пользователь (сотрудник организации) обязан при работе в локальной сети руководствоваться политикой безопасности, выполнять приказы и инструкции, сообщать обо всех инцидентах руководству.

Пользователи персональных компьютеров представляют особый интерес в соблюдении информационной безопасности. Значительная часть информации теряется именно из-за ошибок сотрудников, которые работают с электронно-вычислительной техникой. По своей неосторожности или при небрежном обращении они могут пропускать ошибки в техническом программном обеспечении или вводить неверные данные.

Угроза — это событие или действие, из-за чего может произойти ущерб интересу пользователя.

Основные угрозы следующие:
– компрометирующая информация;
– утечка конфиденциальной информации;
– несанкционированное использование информационных ресурсов;
– нарушение информационной службы;
– неправильное использование информационных ресурсов;
– несанкционированный обмен информацией между абонентами;
– нарушение технических мер по защите информации;
– использование устаревшего программного обеспечения.

Многочисленные условия и причины, при которых возникают вероятность и предпосылки незаконного получения официальной информации, возникают из-за невыполнения функций руководства и сотрудников организации.

Борьба с информационными преступлениями затрудняет работу, потому что в дополнение к халатности

менеджеров и другим проблемам постоянно разрабатываются новые способы и средства захвата информации и уничтожения программного обеспечения. Постоянное обновление и усовершенствование вредоносных программных продуктов затрудняет разработку постоянных и надежных средств защиты информации от них.

Некоторые виды вредоносных программных продуктов:

- троянский конь;
- червь;
- логическая бомба;
- компьютерный вирус;
- захватчик паролей.

Такая классификация не охватывает всех видов возможных угроз данного типа.

Архитектура системы обработки данных (СОД) и технология ее функционирования позволяют преступнику находить или намеренно формировать лазейки для скрытого доступа к информации, а разнообразие даже известных фактов злонамеренных действий дает достаточные основания предполагать, что таких лазеек существует или может образоваться множество.

Преступный доступ бывает прямым и косвенным; первый происходит с физическим воздействием на элементы системы обработки данных, второй, следовательно, напротив.

На данное время существуют различные пути доступа к информации:

- удаленная фотосъемка;
- обеспечение информационной безопасности органов внутренних дел;
- использование удаленных записывающих устройств;
- перехват электромагнитного излучения;
- кража носителей информации;
- копирующий носитель;
- считывание данных;
- маскировка под зарегистрированного пользователя путем кражи паролей;
- применение программных ловушек;
- получение защищенных данных с помощью серии авторизованных запросов;
- использование недостатков языков программирования и операционных систем;
- введение в библиотеку программ особых блоков типа «троянский конь»;
- незаконное подключение к каналам связи вычислительной системы;
- вывод из строя устройств защиты.

Автоматизированная система состоит из основных структурно-функциональных элементов:

- межсетевые мосты;
- сервера или хост-машины;
- рабочие станции;
- каналы связи.

Контроль обработки информации происходит с рабочих станций, запуск программ, корректировка данных. При попытке совершения несанкционированных действий они будут наиболее доступными [22].

Сервера (хост-машины) нуждаются в защите, как и мосты. Первые используются в качестве носителей значительных объемов информации, а вторые — в качестве элементов, где выполняется преобразование данных при координации протоколов обмена в разных частях сети [23].

Средства защиты информации

Средства защиты информации — совокупность различных средств, таких как организационные, технические и правовые, которые направлены на обеспечение информационной безопасности.

Средства обеспечения информационной безопасности подразделяют на две группы:

- формальные — средства, которые выполняют свои функции по защите информации без участия пользователя;
- неформальные — соответственно, с участием пользователя.

Формальные средства, в свою очередь, делятся на физические, аппаратные и программные.

Физические — механические, электрические, электронно-механические устройства и системы, которые работают автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные — схемно встраиваются в аппаратуру системы обработки данных для решения задач по защите информации.

Так, наряду с вышеизложенным, будет проведен ряд мер, необходимых для осуществления защиты информации. К ним относятся следующие:

- распределение и замена деталей контроля доступа (ролей, ключей шифрования и т. д.);
- меры по пересмотру состава и конструкции системы безопасности;
- меры, выполняемые в случае кадровых изменений в штате системы;
- подбор и расстановка персонала (контроль набора, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, организация условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.);
- противопожарная защита, безопасность помещений, контроль доступа, меры по обеспечению сохранности и физической целостности оборудования и носителей данных и т. д.;
- открытая и скрытая проверка работы персонала системы;
- проверка использования мер безопасности;
- меры по пересмотру правил разграничения доступа пользователей к информации в организации;

– другие мероприятия по защите информации, такие как меры технического характера (программные, аппаратные и комплексные) [24].

В ходе изучения этой проблемы было выявлено, что органы внутренних дел уделяют особое внимание сохранности секретной информации, развитию большой бдительности среди сотрудников. Однако некоторые из них часто недооценивают серьезность утечки такой информации. Они проявляют недобросовестное отношение и небрежность при обращении с секретными документами, и это часто приводит к разглашению секретной информации, а иногда к потере секретных продуктов и документов. В то же время уволенные и несогласные с решением руководства сотрудники поддерживают сомнительные связи, разглашают важную информацию о методах и формах работы органов внутренних дел [25].

Низкие профессиональные качества некоторых сотрудников часто приводят к нарушению секретности проводимых мероприятий.

Анонимный биометрический контроль доступа как один из способов защиты информации

Системы контроля доступа, использующие новейшие биометрические технологии, могут обеспечить более высокий уровень безопасности, чем обычные системы, основанные на паролях. Чтобы защитить свои данные, однозначно нужен тяжелый пароль, который является индивидуальным и не будет повторяться ни с одним из существующих паролей, но, как правило, тяжелый пароль можно забыть, что нельзя говорить о сетчатке глаз или отпечатке пальца. Однако их широкое внедрение может серьезно подорвать права людей на неприкосновенность частной жизни. Биометрические сигналы являются неизменяемыми и могут использоваться для привязки личности людей к конфиденциальным личным записям в разрозненных базах данных. Система ABAC (Attribute-Based Access Control) — разграничение доступа на основе атрибутов — использует новые протоколы на основе гомоморфного шифрования (ГШ) (форма шифрования, которая позволяет пользователям выполнять вычисления с зашифрованными данными без их предварительного дешифрования) для проверки членства пользователя, не зная его (ее) истинной личности. Чтобы сделать протоколы на основе немасштабируемых для больших биометрических баз данных, можно предложить платформу анонимного квантования (KAQ), которая обеспечивает эффективный и безопасный компромисс между конфиденциальностью и сложностью. KAQ ограничивает знания сервера о пользователе k максимально разными кандидатами в базе данных, где k контролирует степень компромисса между сложностью и конфиденциальностью. KAQ реализуется путем поиска в таблице с постоянным временем для идентификации кандидатов, за которым следует протокол сопоставления на основе ГШ, применяемый только к этим кандидатам. Защитой конфиденциальности выступает максимальное различие, которое позволяет стереть (уничтожить) любые шаблоны сходства среди возвращенных клиентов. Результаты исследований по биометрии радужной оболочки глаза показали эффективность и достоверность предложенной концепции и описывают практическую реализацию анонимной биометрической концепции.

Ключевым различием между анонимностью при раскрытии данных и сопоставлением биометрических данных является необходимость безопасного сотрудничества между двумя сторонами — биометрическим сервером и пользователем. Формальными исследованиями такой проблемы являются безопасные многопартийные вычисления (SMC) — подобласть криптографии, целью которой является создание методов, позволяющих сторонам совместно вычислять функции по их входам, сохраняя эти входные данные частными и сохраняя независимость и точность вычислений. SMC является одной из наиболее активных областей исследований в области криптографии и имеет широкое применение в электронном голосовании, онлайн-торгах, поиске по ключевым словам и анонимной маршрутизации. Хотя ранее не было работ, использующих SMC для биометрического сопоставления, многие из основных компонентов системы BAS (Breach and Attack Simulation) системы моделирования атак могут быть защищены в рамках этой парадигмы. Они включают следующее: внутренний продукт, полиномиальное вычисление, пороговое значение, медиана, матричное вычисление, логические манипуляции, кластеризация средств, дерево решений и другие классификаторы.

Основным препятствием при применении защищенных в вычислительном отношении протоколов SMC для биометрического сопоставления является их высокая вычислительная сложность. Например, классическое решение проблемы порогового значения (в литературе по SMC эту проблему обычно называют проблемой безопасного миллионера) или сравнения двух частных номеров a и b заключается в использовании передачи без учета (OT). OT — это протокол SMC для совместного поиска в таблице. Гарантией конфиденциальности функции является то, что вся таблица зашифрована с применением предварительно вычисленного набора открытых ключей и передана принимающей стороне. Защита конфиденциальности выбора записи таблицы обеспечивается посредством запутывания правильного открытого ключа среди фиктивных ключей. Даже с учетом недавних достижений в снижении коммуникационной и вычислительной сложности, интенсивные операции шифрования, большой размер таблицы и дешифрования представляют затруднение OT для операций обработки сигналов на уровне выборки или пикселей.

Практичные гомоморфные шифрования, такие как криптосистема Пэйе — вероятностная криптосистема с открытым ключом, изобретенная французским криптографом Паскалем Пэйе (франц.

Pascal Paillier) в 1999 г., — базируется на алгоритме вероятностного асимметричного преобразования и применяется в криптографических протоколах с открытым ключом. В основу криптосистемы положена вычислительная проблема факторизации больших чисел. Могут поддерживать сложение только между двумя зашифрованными числами, но делают это в гораздо большей аддитивной группе открытого текста, обеспечивая тем самым широкий динамический диапазон для вычислений. Кроме того, умножение между зашифрованными номерами может быть выполнено путем рандомизации и взаимодействия между сторонами. В последнее время шифрование Пэйе применяется в ряде фундаментальных строительных блоков обработки сигналов, включая базовые классификаторы и дискретное косинусное преобразование в зашифрованной области. Тем не менее процессы шифрования и дешифрования с открытым ключом в любом гомоморфном шифровании по-прежнему представляют собой серьезное препятствие для преодоления. Например, самый быстрый результат определения порога занимает около 5 секунд для сравнения двух 32-битных чисел с использованием модифицированной системы шифрования Пэйе с размером ключа 1024 бита. Одной из целей этой работы является использование гомоморфного шифрования для построения реалистичной системы сопоставления биометрических данных, которая может обеспечить компромисс между сложностью вычислений и анонимностью пользователя доказуемо безопасным способом.

Говоря об анонимном биометрическом контроле в органах внутренних дел, нужно понимать, что материально-техническое обеспечение находится на недостаточном уровне, соответственно, это затрудняет обеспечение новых видов защиты информации. Для повышения уровня защиты нужно повышать финансирование и повышать квалификацию сотрудников. Можно только представить, как следователь получает информацию по отпечатку пальца или при сканировании лица.

Результаты и обсуждения

Возможные решения проблем информационной безопасности

Решение проблем информационной безопасности стоит перед всеми гражданами и человечеством в целом, государство и отдельные её элементы решают задачи и выполняют функции по защите информации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности, разрабатывает меры по ее обеспечению;
- организует работу органов власти по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;
- организует разработку федеральной программы обеспечения информационной безопасности, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

При решении основных задач и выполнении первоочередных мероприятий государственной политики по обеспечению информационной безопасности в настоящее время доминирует стремление решать главным образом нормативно-правовые и технические проблемы. Чаще всего речь идет о «разработке и внедрении правовых норм», «повышении правовой культуры и компьютерной грамотности граждан», «создании безопасных информационных технологий», «обеспечении технологической независимости» и т. п.

Сочетание программно-технических, законодательных и организационных средств и методов помогут в решении проблем информационной безопасности.

Стоит проблема усовершенствования законодательства в области защиты информации, так как законодательные акты значительно отстают от объективной реальности.

Одна из проблем — это нехватка профессиональных кадров в органах внутренних дел с соответствующим техническим образованием для решения проблем информационной безопасности и расследования киберпреступлений.

Вышеизложенную проблему можно решить следующими способами:

– привлекать специалистов в области работы на электронно-вычислительных машинах к работе в правоохранительных органах;
– вводить курсы по подготовке работы на персональных компьютерах и обеспечению информационной безопасности;
– улучшить финансирование отделов и организаций системы Министерства внутренних дел России для приобретения нового современного высокотехнологичного оборудования, усовершенствования программного обеспечение и операционных систем. Основной причиной является то, что материальная и техническая база, используемая для защиты информации касательно МВД России, находится на низком уровне;
– совершенствовать процесс подготовки соответствующих кадров органов внутренних дел, специализирующихся на защите информации и расследовании преступлений;
– создать для работников благоприятные условия и обеспечить соответствующим денежным довольствием, потому что на данный момент по IT-специальности с финансовой точки зрения работать в частных фирмах или банковской структуре выгоднее.

Программное обеспечение и технические меры важны для обеспечения информационной безопасности. Непрофессиональный сотрудник или устаревшее, нелицензионное программное обеспечение могут послужить источником угрозы.

Соответствующим образом планируется и развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности, то есть преобладает подготовка кадров в области средств связи, обработки информации, технических средств ее защиты. В меньшей степени осуществляется подготовка специалистов в области информационно-аналитической деятельности, социальной информации, информационной безопасности личности. К сожалению, многие государственные институты считают наиболее важной техническую сторону проблемы, упуская из виду социально-психологические ее аспекты.

Заключение

Исходя из статистики, можно говорить о том, что во всех странах ущерб от злоумышленного завладения информацией растет. Существенной причиной является отсутствие системного подхода. Соответственно, нужно улучшить комплексные средства защиты. Важной задачей является организация антивирусной защиты автономных рабочих станций, корпоративных и локальных сетей, которые обрабатывают информацию ограниченного доступа. Шифрование данных, повышение квалификации работников, усовершенствование нормативных правовых актов и соблюдение политики информационной безопасности. Использование новых систем защиты информации как анонимный биометрический контроль данных. Психологический контроль сотрудников и защита информации в самих органах внутренних дел. Важно уделить внимание тому, чтобы при увольнении сотрудники не использовали секретные данные; конечно, это находится под защитой уголовной ответственности, но не всегда правовое сознание помогает защитить данные.

Обеспечение информационной безопасности является комплексной задачей. Это определяется тем, что в информационной среде работают различные компоненты: программное обеспечение, персонал, электронное оборудование.

Чтобы решить данную проблему, важно использование таких мер, как законодательные, организационные и программно-технические. Нельзя пренебрегать хотя бы одним из правил, что может привести к потере информации, которая может понести значительный ущерб.

Использование эффективных информационных систем проявляется как необходимое условие для успешной работы органов внутренних дел Российской Федерации.

Одним из важнейших показателей качества информационных систем является информационная безопасность. Одними из успешных атак являются вирусные атаки. Около 45% инцидентов информационной безопасности и около 55% реализованных угроз от числа зарегистрированных и включенных в статистические обзоры приходится на их долю.

Соблюдение информационной безопасности — это не задача отдельной страны или группы людей, а всего человечества. Быстрое и высокое развитие технологий способствуют помощью хакерам выйти на мировой уровень. Достигнуть эффективной борьбы с ними возможно только при тесном сотрудничестве правоохранительных органов со всего мира. Нужно построить совместный комплекс средств и способов, обучение профессиональных кадров стоит вынести на первое место, необходимо также детально разобрать основу политики безопасности, без которой невозможно нормальное функционирование информационных сетей.

Литература

1. Аверченков В.И. Аудит информационной безопасности органов исполнительной власти : учебное пособие. М. : Флинта, 2020. 297 с.
2. Аверченков В.И. Аудит информационной безопасности : учебное пособие. М. : Флинта, 2021. 679 с.
3. Актуальные киберугрозы: II квартал 2023 года. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 20.08.2023).
4. Шилов А., Мищенко В. Информационная безопасность финансового учреждения. М. : LAP Lambert Academic Publishing, 2021. 164 с.
5. Астахова Л. Герменевтика в информационной безопасности. М. : LAP Lambert Academic Publishing, 2020. 296 с.
6. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : монография. М. : Мир, 2020. 552 с.
7. Баранова Е.К. Информационная безопасность и защита : учебное пособие. М. : РИОР, Инфра-М, 2020. 324 с.
8. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности. М. : Международный гуманитарный фонд «Знание», 2019. 416 с.
9. Бирюков А.А. Информационная безопасность. Защита и нападение. М. : ДМК Пресс, 2021. 474 с.
10. Васильков А.В. Безопасность и управление доступом в информационных системах : учебное пособие. М. : Форум, 2021. 463 с.
11. Галатенко В.А. Стандарты информационной безопасности. М. : Национальный Открытый Университет «ИНТУИТ», 2019. 308 с.
12. Зенков А.В. Информационная безопасность и защита информации : учебное пособие для вузов. М. : Юрайт, 2023. 107 с.
13. Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования. М. : Юрайт, 2023. 342 с.
14. Конституция Российской Федерации // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 13.09.2023).
15. Корабельников С.М. Преступления в сфере информационной безопасности : учебное пособие для вузов. М. : Юрайт, 2023. 104 с.
16. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Под ред. Т.А. Поляковой, А.А. Стрельцова. М. : Юрайт, 2023. 325 с.
17. Положение о Главном управлении собственной безопасности МВД России, утвержденное приказом МВД России от 16 июня 2011 г. № 679 «Об утверждении положения о Главном управлении собственной безопасности Министерства внутренних дел Российской Федерации» // Официальный сайт МВД России. URL: https://мвд.рф
18. Приговор Ленинского районного суда г. Комсомольска-на-Амуре (Хабаровский край) № 1-439/2019 1-47/2020 от 27 мая 2020 г. по делу № 1-439/2019.
19. Приказ ГУ МВД России по г. Москве от 27 апреля 2022 г. № 143 «Об организации эксплуатации сервисов ИСОД МВД России» // Официальный сайт МВД России. URL: https://мвд.рф
20. Суворова Г.М. Информационная безопасность : учебное пособие для вузов. М. : Юрайт, 2023. 253 с.
21. Чернова Е.В. Информационная безопасность человека : учебное пособие для вузов. 2-е изд., испр. и доп. М. : Юрайт, 2023. 243 с.
22. Чернова Е.В. Информационная безопасность человека : учебное пособие для вузов. 3-е изд., перераб. и доп. М. : Юрайт, 2024. 327 с.
23. Зенков А.В. Информационная безопасность и защита информации : учебное пособие для вузов. 2-е изд., перераб. и доп. М. : Юрайт, 2024. 107 с.
24. Суворова Г.М. Информационная безопасность : учебное пособие для вузов. 2-е изд., перераб. и доп. М. : Юрайт, 2024. 277 с.
25. Корабельников С.М. Преступления в сфере информационной безопасности : учебное пособие для вузов. М. : Юрайт, 2024. 111 с.

INFORMATION SECURITY IN RUSSIA'S BODIES OF INTERNAL AFFAIRS: PROBLEMS AND WAYS TO SOLVE THEM

Khasan Karimov, *Ph.D. (Technology), Associate Professor at the Department of Management in Bodies of Internal Affairs of the Ufa Law Institute of Russia's Ministry of Internal Affairs, Ufa, Russian Federation.*
ORCID: 0000-0003-1837-7052, ResearcherID: RIDG-5422-2018.
E-mail: krig.blits@mail.ru

Valerii Permiakov, *Ph.D. (Technology), Associate Professor at the Department of Applied Mechanics and Computer Engineering of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: ir.perm@yandex.ru

Liailia Tarkhova, *Ph.D. (Technology), Associate Professor at the Department of Applied Mechanics and Computer Engineering of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: tarkhova@inbox.ru

Vil' Urmanov, *Ph.D. (Technology), Associate Professor at the Department of Applied Mechanics and Computer Engineering of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: uvg55@mail.ru

Kirill Iuzmukhametov, *4th year student at the Faculty for Investigators' Training of the Ufa Law Institute of Russia's Ministry of Internal Affairs, Ufa, Russian Federation.*
E-mail: mr.kiryt@mail.ru

Insaf Iamilev, *Ph.D. student at the Ufa University of Science and Technology, Ufa, Russian Federation.*
E-mail: yuristyamilev@gmail.com

Dmitrii Gusev, *Ph.D. (Technology), Associate Professor at the Department of Applied Mechanics and Computer Engineering of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: bsau-ngg@yandex.ru

Marat Talypov, *Ph.D. (Biology), Senior Lecturer at the Land Management Department of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: talypovmarat@yandex.ru

Il'nara Bagautdinova, *Ph.D. (Technology), Senior Lecturer at the Department of Applied Mechanics and Computer Engineering of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: isalimyanova@mail.ru

Elizaveta Dik, *Ph.D. (Psychology), Associate Professor at the Department of Mathematics of the Bashkir State Agrarian University, Ufa, Russian Federation.*
E-mail: lizadik@mail.ru

Keywords: *information security, communication technologies, local and global networks, biometric control, cybersecurity, network security, break-in.*

Abstract

Purpose of the study: studying information security problems in Russia's bodies of internal affairs. Together with a rapid development of information and communication technologies, threats arising from failure to comply with elementary rules of using these technologies are also developing. The paper deals with such problems encountered not only by ordinary users but also by officers of bodies of internal affairs.

Methods used in the study: ways for solving the arising problems are put forward. The relevance of this topic is caused by the growth of crime in the information field: theft, break-in, destruction, damage, which requires enhancing the mechanism of protection against these threats. Theoretical aspects of information security in local and global networks are described. Methods of comparison are used. A detailed description of the procedure for using anonymous biometric access control is given.

Study findings: solutions for information security problems encountered by both ordinary users and officers of Russia's bodies of internal affairs are put forward. It is proposed to form a systemic approach to this problem which would be a solution for a number of information security problems. Improving complex protection tools is needed.

References

1. Averchenkov V.I. Audit informatsionnoi bezopasnosti organov ispolnitel'noi vlasti : uchebnoe posobie. M. : Flinta, 2020. 297 pp.
2. Averchenkov V.I. Audit informatsionnoi bezopasnosti : uchebnoe posobie. M. : Flinta, 2021. 679 pp.
3. Aktual'nye kiberugrozy: II kvartal 2023 goda. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2022-q1/ (data obrashcheniia: 20.08.2023).
4. Shilov A., Mishchenko V. Informatsionnaia bezopasnost' finansovogo uchrezhdeniia. M. : LAP Lambert Academic Publishing, 2021. 164 pp.
5. Astakhova L. Germenevtika v informatsionnoi bezopasnosti. M. : LAP Lambert Academic Publishing, 2020. 296 pp.
6. Autentifikatsiia. Teoriia i praktika obespecheniia bezopasnogo dostupa k informatsionnym resursam : monografiia. M. : Mir, 2020. 552 pp.
7. Baranova E.K. Informatsionnaia bezopasnost' i zashchita : uchebnoe posobie. M. : RIOR, Infra-M, 2020. 324 pp.
8. Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Osnovy informatsionno-psikhologicheskoi bezopasnosti. M. : Mezhdunarodnyi gumanitarnyi fond "Znanie", 2019. 416 pp.
9. Biriukov A.A. Informatsionnaia bezopasnost'. Zashchita i napadenie. M. : DMK Press, 2021. 474 pp.
10. Vasil'kov A.V. Bezopasnost' i upravlenie dostupom v informatsionnykh sistemakh : uchebnoe posobie. M. : Forum, 2021. 463 pp.
11. Galatenko V.A. Standarty informatsionnoi bezopasnosti. M. : Natsional'nyi Otkrytyi Universitet "INTUIT", 2019. 308 pp.
12. Zenkov A.V. Informatsionnaia bezopasnost' i zashchita informatsii : uchebnoe posobie dlia vuzov. M. : Iurait, 2023. 107 pp.
13. Kazarin O.V., Shubinskii I.B. Osnovy informatsionnoi bezopasnosti: nadezhnost' i bezopasnost' programmnogo obespecheniia : uchebnoe posobie dlia srednego professional'nogo obrazovaniia. M. : Iurait, 2023. 342 pp.
14. Konstitutsiia Rossiiskoi Federatsii. Ofitsial'nyi internet-portal pravovoi informatsii. URL: http://www.pravo.gov.ru (data obrashcheniia: 13.09.2023).
15. Korabel'nikov S.M. Prestupleniia v sfere informatsionnoi bezopasnosti : uchebnoe posobie dlia vuzov. M. : Iurait, 2023. 104 pp.
16. Organizatsionnoe i pravovoe obespechenie informatsionnoi bezopasnosti : uchebnik i praktikum dlia vuzov. Pod red. T.A. Poliakovoi, A.A. Strel'tsova. M. : Iurait, 2023. 325 pp.
17. Polozhenie o Glavnom upravlenii sobstvennoi bezopasnosti MVD Rossii, utverzhdennoe prikazom MVD Rossii ot 16 iiunia 2011 g. No. 679 "Ob utverzhdenii polozheniia o Glavnom upravlenii sobstvennoi bezopasnosti Ministerstva vnutrennikh del Rossiiskoi Federatsii". Ofitsial'nyi sait MVD Rossii. URL: https://mvd.ru
18. Prigovor Leninskogo raionnogo suda g. Komsomol'ska-na-Amure (Khabarovskii krai) No. 1-439/2019 1-47/2020 ot 27 maia 2020 g. po delu No. 1-439/2019.
19. Prikaz GU MVD Rossii po g. Moskve ot 27 aprelia 2022 g. No. 143 "Ob organizatsii ekspluatatsii servisov ISOD MVD Rossii". Ofitsial'nyi sait MVD Rossii. URL: https://mvd.ru
20. Suvorova G.M. Informatsionnaia bezopasnost' : uchebnoe posobie dlia vuzov. M. : Iurait, 2023. 253 pp.
21. Chernova E.V. Informatsionnaia bezopasnost' cheloveka : uchebnoe posobie dlia vuzov. 2-e izd., ispr. i dop. M. : Iurait, 2023. 243 pp.
22. Chernova E.V. Informatsionnaia bezopasnost' cheloveka : uchebnoe posobie dlia vuzov. 3-e izd., pererab. i dop. M. : Iurait, 2024. 327 pp.
23. Zenkov A.V. Informatsionnaia bezopasnost' i zashchita informatsii : uchebnoe posobie dlia vuzov. 2-e izd., pererab. i dop. M. : Iurait, 2024. 107 pp.
24. Suvorova G.M. Informatsionnaia bezopasnost' : uchebnoe posobie dlia vuzov. 2-e izd., pererab. i dop. M. : Iurait, 2024. 277 pp.
25. Korabel'nikov S.M. Prestupleniia v sfere informatsionnoi bezopasnosti : uchebnoe posobie dlia vuzov. M. : Iurait, 2024. 111 pp.