ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004:056 **DOI: 10.18413/2518-1092-2023-8-4-0-1**

Кальченко Д.М.
Заливин А.Н.
Федоров А.В.

АНАЛИЗ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Белгородский университет кооперации, экономики и права,
ул. Садовая, д. 116а, г. Белгород, 308023, Россия

e-mail: zalivin@bsu.edu.ru

Аннотация
В статье рассмотрены различные средства защиты, которые способны обеспечить безопасность информационных систем (ИС) государственных органов. При рассмотрении средств защиты для обеспечения безопасности информационных систем, важно учитывать возможность успешного внедрения искаженной информации. Это позволяет определить наиболее значимые угрозы и риски для органов власти, чтобы разработать наиболее эффективные меры защиты. Среди рассматриваемых средств защиты будут системы управления доступом, межсетевые экраны, антивирусы, системы обнаружения вторжений и шифрование данных. Каждый из этих инструментов имеет свои особенности и функциональные возможности, которые необходимо изучить и проанализировать. Путем анализа этих средств защиты мы сможем определить, какие из них могут быть наиболее эффективными для обеспечения безопасности информационных систем в различных сценариях. Такой подход позволит государственным органам разрабатывать и внедрять комплексные и адаптированные к своим нуждам стратегии безопасности, минимизируя уязвимости и риски. Так же рассмотрены основные принципы выбора и внедрении средств защиты и предложены основные отечественные системы управления информационной безопасностью, а также необходимые организационные меры после внедрения этих средств. Таким образом, анализ средств защиты для обеспечения безопасности ИС, рассмотренный в статье, предлагает исследование различных инструментов и помогает государственным органам принять обоснованные решения в области безопасности.

Ключевые слова: проблемы информационной безопасности; анализ и выбор программных и аппаратных средств; аппаратные средства защиты; программные средства защиты; замещение импортного программного обеспечения

Для цитирования: Кальченко Д.М., Заливин А.Н., Федоров А.В. Анализ программных и программно-аппаратных средств для защиты информации в информационных системах органов государственной власти // Научный результат. Информационные технологии. – Т.8, №4, 2023. – С. 3-11. DOI: 10.18413/2518-1092-2023-8-4-0-1

Kalchenko D.M.
Zalivin A.N.
Fedorov A.V.

ANALYSIS OF SOFTWARE AND HARDWARE-SOFTWARE TOOLS FOR INFORMATION PROTECTION IN INFORMATION SYSTEMS OF PUBLIC AUTHORITIES

Belgorod University of Cooperation, Economics and Law, 116a Sadovaya str., Belgorod, 308023, Russia

e-mail: zalivin@bsu.edu.ru

Abstract
The article discusses various means of protection that can ensure the security of information systems (IS) of government agencies. When considering security measures to ensure the security of information systems, it is important to consider the possibility of successful implementation of distorted information. This makes it possible to identify the most significant threats and risks for the authorities in order to develop the most effective protection measures. Among the security tools under consideration will be access control systems, firewalls, antiviruses, intrusion detection systems and data encryption. Each of these tools has its own features and functionality that need to be studied and analyzed. By analyzing these security measures, we will be able to determine which of them may be most effective for ensuring the security of information systems in various scenarios. This approach will allow government agencies to develop and implement comprehensive and tailored security strategies, minimizing vulnerabilities and risks. The basic principles of the choice and implementation of security tools are also considered and the main domestic information security management systems are proposed, as well as the necessary organizational measures after the introduction of these tools. Thus, our analysis of IP security protections offers a study of various tools and helps government agencies make informed security decisions.
Keywords: information security problems; analysis and selection of software and hardware; hardware protection; software protection tools; replacement of imported software
For citation: Kalchenko D.M., Zalivin A.N., Fedorov A.V. Analysis of software and hardware-software tools for information protection in information systems of public authorities // Research result. Information technologies. – T.8, №4, 2023. – P. 3-11. DOI: 10.18413/2518-1092-2023-8-4-0-1

ВВЕДЕНИЕ

Для информационных систем (ИС) органов государственной власти проблема информационной безопасности должна стоять на первом плане. Это обусловлено тем фактом, что такие системы обрабатывают конфиденциальную информацию, такую как персональные данные, государственную тайну и другие виды информации. Поэтому защита информации в данных системах становится приоритетной задачей для государства.

Анализ и выбор программных и аппаратных средств являются важным этапом в процессе обеспечения информационной безопасности в ИС органов государственной власти. Главная цель этого этапа - определить эффективность выбранных инструментов для защиты информации от различных угроз и найти оптимальные решения, соответствующие требованиям законодательства Российской Федерации.

К аппаратным средствам относятся различные электронные, электронно-механические и электронно-оптические устройства. Сегодня на рынке представлено огромное их количество, и они имеют разное предназначение. К примеру, существуют специальные реестры, предназначенные для хранения паролей и идентифицирующих кодов, устройства для измерения биометрических показателей человека, таких как голос или отпечатки пальцев, также существуют устройства для шифрования информации, которые основаны на криптографических методах.

Использование аппаратных средств защиты информации в ИС государственных органов позволит провести специальные исследования, которые выявят потенциальные каналы утечки информации и помогут устранить их, а также обеспечат защиту от незаконного доступа к конфиденциальным данным.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Аппаратные средства защиты информации подразделяются на несколько категорий: средства обнаружения, средства поиска, средства детальных измерений и средства активного и пассивного противодействия. Среди средств поиска можно выделить аппаратуру для исследования каналов, в которых может произойти утечка информации и аппаратуру поиска средств съема информации.

Одним из аппаратных средств защиты информации является «eToken». Это устройство обеспечивает двухфакторную аутентификацию и безопасное хранение ключей шифрования. Он может использоваться для доступа к защищенным ресурсам, таким как веб-сайты, приложения и электронные документы, а также для хранения сертификатов и ключей электронной подписи.

Существуют различные модели «eToken». Одни имеют генератор одноразовых паролей, в других сочетается функционал смарт-карты и хранят существенные объемы данных во встроенной флэш-памяти или содержат только генератор одноразовых паролей. Есть модели, которые дают возможность генерировать ключи электронной подписи или могут использоваться для доступа в помещения.

«eToken» используется для аутентификации сотрудников и хранения ключевой информации их можно применять в ИС государственных органов, в которых хранится конфиденциальная информация, так как они рекомендуются к использованию для сертифицированных средств криптографической защиты информации.

Помимо аппаратных устройств защиты, существуют программные средства. Они работают в составе программного обеспечения.

Рассмотрим разновидности программных средств защиты, которые применимы в ИС государственных органов для защиты информации.

Антивирусное программное обеспечение применятся для выявления и уничтожения вирусов и других вредоносных программ. Оно предотвращает распространение вирусов на разные устройства и обеспечивает безопасность операционных систем и данных.

Компьютерные вирусы — это программы, главной целью которых является нарушение работы вычислительной системы, получение доступа к данным или их уничтожение. Некоторые из них остаются постоянно в оперативной памяти. Однако особенность некоторых компьютерных вирусов в том, что они кажутся вполне безобидными, но на самом деле нарушают работу системы. Такие вирусы называются "троянскими конями". Вирусы обладают способностью распространяться внутри компьютера и по сети. Одной из важнейших областей в сфере безопасности является борьба с вирусами и для этой задачи разработано множество инструментов. Некоторые из них работают в режиме сканирования, проверяя содержимое жестких дисков и оперативной памяти компьютера на наличие вредоносных объектов. Другие, должны быть все время активны и находиться в оперативной памяти, где они следят за текущими задачами.

Существует множество разновидностей антивирусного программного обеспечения, таких как «Acronis AntiVirus», «Avast», «Avira AntiVir», «A-square anti-malware», «Dr.Web», «Антивирус Касперского», «eScan Antivirus», «F-Secure», «G-DATA Antivirus», «Graugon Antivirus», «McAfee», «Microsoft Security Essentials», «NOD 32», «Norman Virus Control», «Norton AntiVirus и другие.

В качестве рекомендаций можно привести несколько методов, которые помогают противодействовать компьютерным вирусам и уменьшать возможный ущерб от их заражения. Первый, это профилактика и уменьшение ущерба, который включает в себя регулярное обновление операционной системы и программного обеспечения, установку надежного антивирусного программного обеспечения с возможностью обнаружения и удаления известных вирусов, а также ограничение доступа к ненадежным веб-сайтам и подозрительным файлам. А второй, это метод обнаружения и удаления неизвестных вирусов, который включает анализ поведения программ и процессов на компьютере для обнаружения подозрительной активности, использование антивирусных программ, способных обнаруживать и удалять новые, еще неизвестные вирусы, а также осуществление резервного копирования данных, чтобы обеспечить возможность восстановления объектов, которые могут быть поражены вирусами.

Таким образом, предпринимаются меры профилактики заражения компьютера, а также разрабатываются и применяются антивирусные программы для определения и удаления как известных, так и неизвестных вирусов. В случае инфицирования важно помнить о восстановлении пораженных объектов с помощью резервных копий.

Виртуальное пространство Интернета является главным источником заражения вирусами, особенно при обмене электронными письмами.

Иногда пользователь зараженный вирусом файл неосознанно направляет адресатам, которые перенаправляют новые зараженные электронные письма и это вызывает массовое заражение компьютерной техники. Из этого следует, что необходимо исключать контакты с неизвестными источниками информации и использовать только лицензионное программное обеспечение.

Для обеспечения информационной безопасности в ИС государственных органов можно применять механизмы шифрования данных. Криптографические методы защиты информации используются для обработки, хранения и передачи информации по сетям связи. Криптография представляет собой науку о методах преобразования информации для ее защиты и включает в себя алгоритмы шифрования, ключи шифрования и методы аутентификации. Она используется для обеспечения конфиденциальности, целостности и аутентификации данных.

Шифрование – это процесс преобразования данных в непонятную форму для человека и программных комплексов, которая недоступна для чтения без ключа шифрования-расшифровки. Криптографические методы защиты информации являются важной составляющей концепции информационной безопасности, обеспечивая конфиденциальность данных и защищая их в процессе передачи по сети.

Ключ – это последовательность символов, которая определяет алгоритмы шифрования и дешифрования для обеспечения информационной безопасности. Локальные сети должны обеспечивать не только конфиденциальность, но и целостность данных, то есть предотвращать изменение и повреждение данных во время их передачи и хранения. Для обеспечения целостности данных необходимы инструменты, способные обнаруживать любые изменения в исходных данных.

При проведении аудита ИС государственных органов, большое внимание необходимо уделять возможности успешного внедрения искаженной информации. Однако криптография способна сократить эту вероятность до незначительного уровня.

Вот некоторые средства криптозащиты: «Signal-COM Cloud DSS Client», «Secret Disk», «ЛИРССЛ-CSP», криптопровайдер «КриптоПро CSP», «КриптоПро JCP», «ViPNet Client», «ViPNet CSP», «ViPNet CryptoFile», «ViPNet SafeDisk», «КриптоАРМ», «Континент».

Идентификация и аутентификация являются незаменимыми составляющими информационной безопасности для ИС государственных учреждений. Перед предоставлением доступа к ИС пользователи должны пройти ряд процедур, обеспечивающих защиту и контроль доступа:

- идентификацию – это процесс определения личности человека, который пытается получить доступ к ИС. Обычно для этого необходимо ввести имя пользователя или другой идентификатор;
- аутентификацию – это процедура подтверждения того, что пользователь или система являются действительно теми, за кого себя выдают. Этот процесс может осуществляться различными способами, такими как пароли, безопасные токены, использование биометрических данных и другие.

Существуют две формы представления объектов, выполняющих аутентификацию пользователей, это внешняя и внутренняя.

Объект аутентификации, находящийся вне системы, может быть самостоятельным устройством (например, ключ-карты), или это может быть внешнее программное обеспечение, взаимодействующее с ИС по протоколу аутентификации (например, OAuth, SAML).

Внутренний объект аутентификации, являющийся частью ИС, представляет собой модуль или компонент системы, который принимает информацию от внешнего объекта и выполняет процедуру аутентификации пользователя. Этот внутренний объект может проверять данные пользователя, сверять их с информацией, которая хранится в ИС или с использованием других методов проверки.

В любом случае, смысл этих объектов состоит в подтверждении идентичности пользователя перед предоставлением доступа к ИС. Однако внешний объект не имеет доступа к ИС и требует внутреннего объекта для проверки и аутентификации пользователей.

Межсетевые экраны, также известные как брандмауэры, широко применяются для обеспечения безопасности компьютерных сетей от внешних угроз. Они работают на основе определенных правил и политик безопасности, которые определяют, какие типы трафика будут разрешены, а какие запрещены. Они также могут выполнять функции «NAT» (Network Address Translation) и «VPN» (Virtual Private Network), обеспечивая защиту и конфиденциальность данных.

Основные преимущества при использовании межсетевых экранов:

- защита от внешних угроз: помогают обеспечить безопасность сети, блокируя несанкционированный доступ и атаки извне. Они просматривают весь трафик, проходящий через сеть, и блокируют вредоносные пакеты данных;
- фильтрация трафика: могут фильтровать трафик на основе различных параметров, например IP-адрес, порт, протокол. Это позволяет ограничить доступ к определенным приложениям или сервисам, а также блокировать небезопасные или нежелательные запросы;
- управление политиками безопасности: позволяют создавать и управлять политиками безопасности, определяющими, какие действия и подключения разрешены в сети. Это обеспечивает гибкость и контроль над сетевым трафиком;
- отслеживание и регистрация событий: могут вести журнал событий, записывая информацию о входящем и исходящем трафике. Это помогает в анализе и отслеживании возможных угроз.

Вот некоторые виды межсетевых экранов: «Solar Next Generation Firewall», «InfoWatch ARMA Industrial Firewall», «Positive Technologies Application Firewall» (PT AF), коммуникационный центр «ИВК КОЛЬЧУГА-К», «Ashampoo FireWall Pro», «AVG Internet Security», «Kaspersky», «Microsoft ISA Server», «Norton, Outpost», «Windows Firewall», «Sunbelt»), аппаратные («Fortinet, Cisco», «Check Point»), «Linux» («Netfilter», «Firestarter», «NuFW», «Uncomplicated Firewall»).

Управление трафиком между локальными и глобальными сетями может осуществляться при помощи Proxy-серверов, которые выполняют роль посредника. При этом, все данные, передаваемые между этими сетями на сетевом и транспортном уровнях, полностью запрещены и не направляются по маршруту. Вместо этого, обращения из локальной сети в глобальную выполняются с применением специальных серверов-посредников. Однако этот метод не является достаточно безопасным на более высоких уровнях, таких как уровень приложений.

Важно учитывать, что к ИС может быть получен несанкционированный доступ к информации. Чтобы предотвратить это, применяются средства защиты информации от несанкционированного доступа.

Это программные комплексы, которые позволяют подключать аппаратные идентификаторы и гарантировать защиту от попыток несанкционированного доступа как для отдельных устройств, так и в составе локальной сети.

Использование средств защиты информации от несанкционированного доступа для ИС государственных органов позволит придерживаться требований законодательства, а также соответствовать стандартам и руководящим документам.

Рассмотрим примеры различных средств, которые можно применить в ИС государственных органов для обеспечения безопасности и предотвращения несанкционированного доступа: «Dallas Lock», «Secret Net Studio», «АПКШ Континент», Аппаратно-программный модуль «Соболь», «Страж NT».

Также для предотвращения несанкционированного доступа в ИС можно использовать системы обнаружения вторжений. Это программные продукты, которые анализируют сетевой трафик и системные журналы с целью обнаружения любой аномальной активности и предупреждают о несанкционированном доступе или взломе системы. Они информируют администраторов о возможных подозрительных действиях и помогают устранять угрозы.

Проведенный анализ разновидностей программного и аппаратного обеспечения для защиты информации в ИС государственных органов показал, что на сегодняшний день существует

множество различных средств, предназначенных для обеспечения безопасности данных. При выборе оптимального метода защиты информации необходимо учитывать несколько факторов, таких как тип данных, которые необходимо защитить, существующие угрозы безопасности в организации и требования законодательства. Кроме того, необходимо оценить эффективность, затраты и совместимость различных средств защиты с уже существующими системами.

Однако только лишь комплексная защита информации способна эффективно предотвратить хищение данных, так как управление ею требует больше, чем простое удаленное управление антивирусами или другими средствами защиты.

В связи с обновлением Доктрины информационной безопасности Российской Федерации, государство рассматривает новые перспективы в развитии инновационных информационных технологий с использованием отечественного программного обеспечения, а также нацелено на усовершенствование системы защиты от угроз информационной безопасности с помощью новых подходов и решений.

С 1 января 2016 г. действует Постановление Правительства Российской Федерации, которое направлено на замещение импортного программного обеспечения на отечественное до конца 2024 года. Это касается всех органов власти, а также бюджетных организаций, осуществляющих государственные закупки.

Для этой цели был создан «Единый реестр российских программ для электронных вычислительных машин и баз данных». Он позволяет расширять использование отечественных программ, подтверждать их происхождение из Российской Федерации и предоставлять правообладателям электронно-вычислительных программ меры государственной поддержки.

Учитывая, что законодательство Российской Федерации ограничивает приобретение иностранных средств защиты информации с целью перехода на отечественные, необходимо понимать, что начальный этап внедрения потребует значительных финансовых и трудовых затрат.

Как примером комплексной системы защиты информации для ИС государственных органов можно предложить следующие решения, которые в совокупности совместимы с отечественной операционной системой «Astra Linux Special Edition» с базовым уровнем защищенности:

- для обнаружения и удаления вирусов применять антивирусное программное обеспечение «DrWeb» или «Антивирус Касперского»;
- при передаче информации по каналам связи и обеспечения ее защиты, возможно использовать программно-аппаратный комплекс VipNet координатор и программное обеспечение «VipNet» клиент. Для развертывания и администрирования сети «VipNet» использовать «VipNet» администратор;
- для обеспечения защиты информации от несанкционированного доступа, использовать программное обеспечение «SecretNet Studio»;
- для проведения оценки состояния защищенности IT-инфраструктуры применять программное обеспечение «XSpider».

В случае необходимости взаимодействия и передачи данных по открытым каналам связи с учреждениями, у которых отсутствует возможность использовать программные или программно-аппаратные комплексы «VipNet», как альтернативу, можно использовать программное обеспечение «КриптоАРМ».

Предлагаемая комплексная система защиты информации имеет несколько ключевых особенностей, которые позволяют ей соответствовать требованиям законодательства Российской Федерации:

- защита персональных данных: система обеспечивает надежную защиту персональных данных, соблюдая все требования Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». Она предоставляет необходимые механизмы для обработки и хранения персональных данных согласно законодательству;
- защита конфиденциальности: система обеспечивает конфиденциальность информации путем шифрования данных и контроля доступа. Она предоставляет механизмы и инструменты для

управления правами доступа к информации и принятия мер по предотвращению несанкционированного доступа.

- защита от внешних атак: система включает в себя мощные механизмы фильтрации и обнаружения вторжений, вирусов и вредоносного ПО. Она способна обнаружить и предотвратить атаки, поддерживать целостность данных и предупреждать о возможных угрозах.

ЗАКЛЮЧЕНИЕ

Таким образом, предлагаемая комплексная система защиты информации обеспечивает соответствие требованиям законодательства Российской Федерации и может быть внедрена с минимальными финансовыми затратами.

На завершающем этапе необходимо помнить, что проведение регулярных обучений и тренингов по информационной безопасности поможет сотрудникам органов власти осознать важность соблюдения правил и процедур, связанных с защитой данных. Их необходимо ознакомить с основными принципами безопасности, такими как использование сложных паролей, установка обновлений на компьютерах и программном обеспечении, правилам обращения с электронной почтой и веб-сайтами.

Кроме того, создание культуры безопасности на рабочих местах является ключевым фактором успеха. Коллективное сознание о важности безопасности должно быть в каждом сотруднике, чтобы они сами были заинтересованы в соблюдении правил и процедур безопасности.

Список литературы

1. ГОСТ Р 50922-96 Защита информации. Основные термины и определения.
2. Об информации, информационных технологиях и защите информации [Электронный ресурс]: федер. закон от 27.07.2007 № 149-ФЗ (ред. от 02.12.2019) // Консультант: сайт информ. – правовой компании – Москва, 2019. – Режим доступа: http://www.consultant.ru/document /cons_doc_LAW_61798// (дата обращения: 30.10.2023).
3. О персональных данных [Электронный ресурс] федер. закон от от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) // Консультант: сайт информ. – правовой компании – Москва, 2019. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801// (дата обращения: 30.10.2023).
4. Стрельцов, А.А. Содержание понятия «обеспечение информационной безопасности». – Текст: непосредственный // Информационное общество, 2015. – №4. – С.12.
5. Бабаш, А.В. Криптографические методы защиты информации: учебное пособие / А.В. Бабаш, Е.К. Баранова. — Москва: Кнорус, 2018. — 190 с. – Текст: непосредственный.
6. Козлов, С.Н. Защита информации: устройства несанкционированного съема и борьба с ними: учебное пособие / С.Н. Козлов. – М.: Академический проект, 2018. – 286 с. – Текст: непосредственный.
7. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Москва: Феникс, 2017. – 348 с. – Текст: непосредственный.
8. Никифоров, С.Н. Методы защиты информации: защищенные сети: учебное пособие / С.Н. Никифоров. – Москва: Лань, 2018. – 96 с. – Текст: непосредственный.
9. Никифоров, С.Н. Методы защиты информации: пароли, скрытые, шифрование: учеб. для вузов / С.Н. Никифоров. – Москва: Лань, 2018. – 124 с. – Текст: непосредственный.
10. Петраков, А.В. Основы практической защиты информации: учебное пособие / А.В. Петраков. – Москва: Солон-пресс, 2005. – 384 с. – Текст: непосредственный.
11. Северин, В.А. Комплексная защита информации на предприятии: учебник для вузов / В.А. Северин. – Москва: Городец, 2008. – 368 с. – Текст: непосредственный.
12. Хорев, П.Б. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. – Москва: Форум, 2019. – 352 с. – Текст: непосредственный.

13.Царегородцев, А.В. Методы и средства защиты информации в государственном управлении: учебное пособие / А.В. Царегородцев, М.М. Тараскин. – Москва: Проспект, 2017. – 208 с. – Текст: непосредственный.

14.Чефранова, А.О. Система защиты информации: курс лекций / А.О. Чефранова. – Москва: ДМК-пресс, 2015. – 392 с. – Текст: непосредственный.

15.Шаньгин, В.Ф. Информационная безопасность и защита информации: учебник для вузов / В.Ф. Шаньгин. – Москва: ДМК-пресс, 2017. – 702 с. – Текст: непосредственный.

16.Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях: учебник для вузов / В.Ф. Шаньгин. – Москва: ДМК-пресс, 2012. – 592 с. – Текст: непосредственный.

17.Модель безопасности AstraLinux — основа для апробации новых ГОСТов – 14.05.2021 г.: статья − URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/– Текст: электронный.

18.С. Шиляев. Проблемы информационной безопасности: алгоритм построения системы ИБ с нуля – 24.02.2015 г.: статья − URL: https://kontur.ru/articles/1622– Текст: электронный.

19.Реестр российского программного обеспечения. Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. − URL: https://reestr.digital.gov.ru/

20.Указ Президента Российской Федерации от 01.05.2022 г. № 250 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации. − URL:http://www.kremlin.ru/acts/bank/47796 – Текст: электронный.

References

1. GOST R 50922-96 Information protection. Basic terms and definitions.

2. About information, information technologies and information protection [Electronic resource]: feder. Law No. 149-FZ of 27.07.2007 (as amended on 02.12.2019) // Consultant: inform. – legal company website – Moscow, 2019. – Access mode: http://www.consultant.ru/document /cons_doc_LAW_61798// (accessed: 10/30/2023)

3. About personal data [Electronic resource] feder. law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) // Consultant: inform. – legal company website – Moscow, 2019. – Access mode: http://www.consultant.ru/document/cons_doc_LAW_61801 // (accessed: 10/30/2023).

4. Streltsov, A.A. The content of the concept of "ensuring information security". – Text: direct // Information Society, 2015. – No.4. – p.12.

5. Babash, A.V. Cryptographic methods of information protection: a textbook / A.V. Babash, E.K. Baranova. — Moscow: Knorus, 2018. — 190 p. – Text: direct.

6. Kozlov, S.N. Information protection: unauthorized removal devices and the fight against them: a textbook / S.N. Kozlov. – M.: Academic project, 2018. – 286 p. – Text: direct.

7. Krakovsky, Yu.M. Information protection: a textbook / Yu.M. Krakovsky. – Moscow: Phoenix, 2017. – 348 p. – Text: direct.

8. Nikiforov, S.N. Methods of information protection: secure networks: a textbook / S.N. Nikiforov. – Moscow: Lan, 2018. – 96 p. – Text: direct.

9. Nikiforov, S.N. Methods of information protection: passwords, hidden, encryption: textbook. for universities / S.N. Nikiforov. – Moscow: Lan, 2018. – 124 p. – Text: direct.

10.Petrakov, A.V. Fundamentals of practical information protection: a textbook / A.V. Petrakov. – Moscow: Solon Press, 2005. – 384 p. – Text: direct.

11.Severin, V. A. Complex information protection at the enterprise: textbook for universities / V.A. Severin. – Moscow: Gorodets, 2008. – 368 p. – Text: direct.

12.Khorev, P.B. Hardware and software protection of information: textbook. the manual / P.B. Khorev. – Moscow: Forum, 2019. – 352 p. – Text: direct.

13.Tsaregorodtsev, A.V. Methods and means of information protection in public administration: a textbook / A.V. Tsaregorodtsev, M.M. Taraskin. – Moscow: Prospekt, 2017. – 208 p. – Text: direct.

14. Chefranova, A.O. Information security system: a course of lectures / A.O. Chefranova. – Moscow: DMK-press, 2015. – 392 p. – Text: direct.

15. Shangin, V.F. Information security and information protection: textbook for universities / V.F. Shangin. – Moscow: DMK-press, 2017. – 702 p. – Text: direct.

16. Shangin, V.F. Information protection in computer systems and networks: textbook for universities / V.F. Shangin. – Moscow: DMK-press, 2012. – 592 p. – Text: direct.

17. The AstraLinux security model is the basis for testing new GOST standards – 05/14/2021: article − URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/ – Text: electronic.

18. S. Shilyaev. Information security problems: an algorithm for building an information security system from scratch – 02/24/2015: article − URL: https://kontur.ru/articles/1622 – Text: electronic.

19. The registry of Russian software. The Ministry of Digital Development, Communications and Mass Media of the Russian Federation. − URL: https://reestr.digital.gov.ru/

20. Decree of the President of the Russian Federation No. 250 dated 05/01/2022 On Additional Measures to Ensure Information Security of the Russian Federation. − URL: http://www.kremlin.ru/acts/bank/47796 – Text: electronic.

Кальченко Даниил Михайлович, магистрант 2 курса кафедры информационной безопасности
Заливин Александр Николаевич, кандидат технических наук, доцент кафедры информационной безопасности
Федоров Алексей Васильевич, магистрант 2 курса кафедры информационной безопасности

Kalchenko Daniil Mikhailovich, 2nd year Master's student of the Department of Information Security
Zalivin Aleksandr Nikolaevich, Candidate of Technical Sciences, associate Professor of the Department of Information Security
Fedorov Alexey Vasilyevich, 2nd year Master's student of the Department of Information Security