Приложение 1
к приказу № 20 – О
от «20» июля 2022

УПРАВЛЕНИЕ ДЕЛАМИ ВОРОНЕЖСКОЙ ОБЛАСТИ

КАЗЕННОЕ УЧРЕЖДЕНИЕ ВОРОНЕЖСКОЙ ОБЛАСТИ «ГОСУДАРСТВЕННЫЙ АРХИВ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОЙ ИСТОРИИ ВОРОНЕЖСКОЙ ОБЛАСТИ» (КУВО «ГАОПИ ВО»)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КУ ВО «ГОСУДАРСТВЕННЫЙ АРХИВ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОЙ ИСТОРИИ ВОРОНЕЖСКОЙ ОБЛАСТИ»

Воронеж
2022

СОДЕРЖАНИЕ

1. Перечень используемых сокращений

АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
БД – База данных.
ЗИ – Защита информации.
ИБ – Информационная безопасность.
ИОК – Инфраструктура открытых ключей.
ИС – Информационная система.
ИТС – Информационно-телекоммуникационная система.
КЗ – Контролируемая зона.
ЛВС – Локальная вычислительная сеть.
МЭ – Межсетевой экран.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПО – Программное обеспечение.
СВТ – Средства вычислительной техники.
СЗИ – Средство защиты информации.
СКЗИ – Средство криптографической защиты информации.
СПД – Система передачи данных.
СУБД – Система управления базами данных.
СУИБ – Система управления информационной безопасностью.
СЭД – Система электронного документооборота.
УЦ – Удостоверяющий центр.
ЭВМ – Электронная – вычислительная машина, персональный компьютер.
ЭП – Электронная подпись.
FTP – File Transfer Protocol.
LDAP – Lightweight Directory Access Protocol.
VPN – Virtual Private Network.

2. Перечень используемых терминов и определений

АВТОМАТИЗИРОВАННАЯ СИСТЕМА – см. ИНФОРМАЦИОННАЯ СИСТЕМА.

АДМИНИСТРАТИВНАЯ СЕТЬ – ЛВС, используемая для настройки и управления активным сетевым оборудованием корпоративной сети и сетевыми средствами защиты информации.

АДМИНИСТРАТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – работник или группа работников отдела Организации, осуществляющие контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

АДМИНИСТРАТОР СЕТИ – работник или группа работников службы технической поддержки, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

ВНУТРЕННЯЯ СЕТЬ – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и ДМЗ межсетевым экраном. Внутренняя сеть объединяет производственные, тестовые, административные сети и сети разработчиков.

ДЕМИЛИТАРИЗОВАННАЯ ЗОНА (ДМЗ) – участок корпоративной сети, расположенный между внешним МЭ и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет). В ДМЗ размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности не целесообразно размещать во внутренней сети КУ ВО «Государственный архив общественно-политической истории Воронежской области».

ДОСТУП К ИНФОРМАЦИИ – возможность получения информации и ее использования.

ДОСТУПНОСТЬ ИНФОРМАЦИИ – состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

ЗАЩИЩЕННЫЙ КАНАЛ ПЕРЕДАЧИ ДАННЫХ – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

ИДЕНТИФИКАТОР ДОСТУПА – уникальный признак субъекта или объекта доступа.

ИДЕНТИФИКАЦИЯ – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИНФОРМАЦИЯ – сведения (сообщения, данные) независимо от формы их представления.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах организации.

ИНФОРМАЦИОННАЯ СРЕДА – совокупность информационно-телекоммуникационной системы, процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных

систем, обеспечивающего автоматизацию КУ ВО «Государственный архив общественно-политической истории Воронежской области».

ИНФОРМАЦИОННАЯ СИСТЕМА – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения бизнес задач подразделений. В КУ ВО «Государственный архив общественно-политической истории Воронежской области» используются различные типы информационных систем для решения производственных, управленческих, учетных и других бизнес задач.

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию бизнес-процессов КУ ВО «Государственный архив общественно-политической истории Воронежской области», и средства защиты информации.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

ИНФОРМАЦИОННЫЕ АКТИВЫ – информационные системы, информационные средства, информационные ресурсы.

ИНФОРМАЦИОННЫЕ СРЕДСТВА – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

КРИТИЧНАЯ ИНФОРМАЦИЯ – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений КУ ВО «Государственный архив общественно-политической истории Воронежской области», привести к причинению материального или иного вида ущерба.

КРИПТОПРОВАЙДЕР – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

МЕЖСЕТЕВОЙ ЭКРАН (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) - доступ к информации, нарушающий установленные правила разграничения доступа.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ (ДАЛЕЕ НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

ОПЕРАЦИОННАЯ СИСТЕМА – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

ОТВЕТСТВЕННОЕ ЛИЦО (АДМИНИСТРАТОР) ИНФОРМАЦИОННЫХ АКТИВОВ – работник КУ ВО «Государственный архив общественно-политической истории Воронежской области», получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе

Примечание: Понятия «Ответственное лицо (администратор) информационных активов и «владелец информационных средств (ресурсов)» идентичны.

ПАРОЛЬ – идентификатор субъекта доступа, который является его (субъекта) секретом.

ПЕРИМЕТРАЛЬНОЕ СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

ПОЛЬЗОВАТЕЛЬ ЛВС – работник (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ – совокупность прикладных программ, установленных на сервере или ЭВМ.

РАБОЧАЯ СТАНЦИЯ – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

РЕГИСТРАЦИОННАЯ (УЧЕТНАЯ) ЗАПИСЬ ПОЛЬЗОВАТЕЛЯ – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.).

Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

РОЛЬ – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

СЕРВЕР – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

СЕТЕВЫЕ (ИНФОРМАЦИОННЫЕ) СЕРВИСЫ – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTPS, Telnet, и другие.

СПИСОК КОНТРОЛЯ ДОСТУПА (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ (СП) – структурное подразделение КУ ВО «Государственный архив общественно-политической истории Воронежской области» с самостоятельными функциями, задачами и ответственностью.

УЗЕЛ – совокупность ЛВС, расположенных в пределах одной контролируемой зоны.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

ЭВМ – электронная – вычислительная машина, персональный компьютер.

ЭЛЕКТРОННАЯ ПОДПИСЬ – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3. Вводные положения

Политика информационной безопасности КУ ВО «ГАОПИ ВО» (далее – Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (далее – ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

Основными целями настоящей Политики являются защита информации Учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Руководители структурных подразделений Учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Работники Учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

Задачами настоящей Политики являются:

1) описание имеющейся в Учреждении системы управления ИБ;

2) определение Политики ИБ Учреждения, а именно:

– политики реализации антивирусной защиты;

– политики реализации контроля доступа;

– политики предоставления доступа к информационному ресурсу;

– политики использования информационного ресурса в рамках существующих информационных систем;

– политики безопасности электронной почты и использования Интернет;

– политики использования паролей;

– политики защиты автоматизированных рабочих мест (далее – АРМ);

– определение порядка сопровождения информационных систем (далее – ИС) Учреждения.

Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его работниками. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

Настоящая Политика вводится в действие и признается утратившей силу Приказом по Учреждению.

Инициаторами внесения изменений в настоящую Политику являются структурные подразделения Учреждения. Плановая актуализация настоящей Политики производится ежегодно. Внеплановая актуализация настоящей Политики производится в обязательном порядке в следующих случаях:

– при внесении существенных изменений в типовую конфигурацию программно-аппаратных средств локальной вычислительной сети Учреждения;

– при изменении политики РФ в области ИБ, указов и законов РФ в области защиты информации;

– при изменении категорий обрабатываемой информации в локальной вычислительной сети Учреждения;

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Учреждения;

– при изменении условий эксплуатации локальной вычислительной сети Учреждения.

Ответственность за актуализацию настоящей политики (плановую и внеплановую) несет администратор ИБ Учреждения.

Контроль за исполнением требований настоящей политики и поддержанием его в актуальном состоянии возлагается на администратора ИБ.

4. Назначение и общая характеристика политики ИБ

Политика ИБ Учреждения – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Учреждении.

Под политикой ИБ понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики ИБ относятся к административным мерам обеспечения информационной безопасности, и определяют стратегию Учреждения в области ИБ.

Политики ИБ регламентируют эффективную работу средств защиты информации. Они охватывает все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях, реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики ИБ, утверждаются руководителем Учреждения.

Правовую основу Политики ИБ составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, локальные нормативные акты Учреждения в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

Ответственность за разработку мер и контроль над обеспечением защиты информации несет администратор информационной безопасности.

Ответственность за реализацию Политик возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;

– в части, касающейся доведения правил Политик до работников Учреждения, а также иных лиц – на руководство Учреждения и руководителей его структурных подразделений;

– в части, касающейся исполнения правил Политики, – на каждого работника Учреждения, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

Организация просвещения работников Учреждения в области ИБ возлагается на администратора информационной безопасности.

Обучение работников Учреждения правилам обращения с информацией, составляющей коммерческую тайну, проводится путем самостоятельного изучения работниками локальных нормативных актов Учреждения, регламентирующих вопросы защиты информации.

Правила допуска к работе с информационными ресурсами лиц, не являющихся работниками Учреждения, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

5. Защищаемые информационные ресурсы

Различаются следующие категории информации, подлежащих защите в Учреждении:

– конфиденциальная – информация, определенная Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– публичная – информация, получаемая из публичных источников (публикации в СМИ, теле– и радиовещание и т.д.);

– открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят;

– ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Информация ограниченного доступа представляет собой сведения, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

К информации ограниченного доступа не могут относиться сведения:

– содержащиеся в учредительных документах Учреждения, документах, подтверждающих факт внесения записей о юридических лицах в соответствующие государственные реестры;

– о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке,

безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования Учреждения, безопасности каждого гражданина и безопасности населения в целом;

– о численности, составе работников, системе оплаты труда, об условиях труда, в том числе об охране труда, показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

– о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

– о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

– о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

– обязательность раскрытия которых, или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Подходы к решению проблемы защиты информации, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования Учреждения.

Для этого в Учреждении выполняются следующие мероприятия:

– определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;

– разрабатываются правила категорирования информации, позволяющие относить ее к различным видам конфиденциальных сведений и определять степень ее критичности для Учреждения;

– устанавливается круг лиц и порядок доступа к подобной информации; вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

– включаются в трудовые договоры с работниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых с другими организациями.

6. Организация и реализация системы управления ИБ

СУИБ – часть общей системы управления Учреждения, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ.

Для успешного функционирования СУИБ Учреждения должны быть реализованы следующие процессы:

– определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ;

– определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Учреждения, а также оценки репутационных и правовых рисков деятельности Учреждения;

– анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов;

– выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;

– принятие руководителями Учреждения остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Учреждения и оценено их влияние на достижение целей его деятельности.

В СУИБ должны быть реализованы следующие процессы:

– разработка плана обработки рисков ИБ;

– реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

– реализация программ по обучению и осведомленности ИБ;

– обнаружение и реагирование на инциденты безопасности;

– обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяются политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Руководством Учреждения принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

7. Методы оценивания информационных рисков

Оценка информационных рисков Учреждения выполняется по следующим основным этапам:

– идентификация и количественная оценка информационных ресурсов, значимых для бизнеса;

– оценивание возможных угроз;

– оценивание существующих уязвимостей;

– оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что уязвимые информационные ресурсы Учреждения подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризует опасность, которой могут подвергаться компоненты корпоративной системы Internet/Intranet.

При этом информационные риски Учреждения зависят от:

– показателей ценности информационных ресурсов;

– вероятности реализации угроз для ресурсов;

– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности Учреждения.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса Учреждения.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

– привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

– возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

– техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

– степенью легкости, с которой уязвимость может быть использована.

8. Политика реализации антивирусной защиты

Настоящая Политика определяет основные средства для реализации антивирусной защиты Учреждения.

Средства антивирусной защиты выполняют функции по ограничению распространения вирусной атаки и ее локализации.

В состав средств антивирусной защиты входят следующие компоненты:

– средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;

– средства антивирусной защиты серверов ЛВС;

– средства антивирусной защиты рабочих станций;

– средства антивирусной защиты почтовой системы (внутренних почтовых серверов и SMTP-шлюзов на внешнем периметре сети);

– антивирусный шлюз, осуществляющий антивирусный контроль HTTPS и FTP трафика.

В качестве средств антивирусной защиты в Учреждении применяются Kaspersky Internet Security.

9. Политика реализации контроля доступа

Настоящая Политика определяет основные правила и средства для организации идентификации/аутентификации пользователей информационных ресурсов Учреждения.

Идентификация и аутентификация должна быть реализована посредством комплекса программно-технических средств, обеспечивающих идентификацию пользователей ИС Учреждения и подтверждение подлинности пользователей при получении доступа к информационным ресурсам.

Функции идентификации и аутентификации выполняются следующими компонентами ИС Учреждения:

– компонентами, встроенными в ОС Windows 7, Windows 10, Windows Server 2012R2;

– оборудованием и ПО, поддерживающим надежные методы;

– аутентификации;

– компонентами СУБД и приложений, которые обеспечивают управление идентификационными данными пользователей, паролями и ключевой информацией.

10. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления работникам доступа к информационным ресурсам Учреждения.

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей Политикой.

Каждому работнику ИС Учреждения, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в ИС.

В случае производственной необходимости некоторым работникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими работниками при работе в ИС Учреждения одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

Процедура регистрации (создания, изменения, прекращения) учетной записи, для работника Учреждения инициируется заявкой начальника подразделения Учреждения, в котором работает данный работник (Приложение 1).

В заявке указывается:

– должность (с полным наименованием подразделения), фамилия, имя и отчество работника;

– основание для регистрации учетной записи (номер приказа о принятии на работу в Учреждение или иного договорного документа, определяющего необходимость предоставления работнику доступа к информационным ресурсам Учреждения).

Заявку подписывает руководитель структурного подразделения (далее – СП), в котором числится работник согласно штатному расписанию (для работников, не входящих в штат Учреждения – руководитель СП курирующего соответствующие договорные отношения), утверждая тем самым производственную необходимость регистрации данного работника в ИС Учреждения.

Администратор ИБ рассматривает представленную заявку, и принимает ее к исполнению или передает ее на исполнение работникам сервисной организации, осуществляющей администрирование ИС Учреждения.

На основании заявки (задания) администратор ИБ совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к сетевым ресурсам ИС Учреждения, таких как право регистрации на АРМ работника и пользования корпоративной электронной почтой.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) учетная запись должна немедленно блокироваться.

Заблокированные учетные записи должны сохраняться в системе не менее 5 лет с момента прекращения срока действия полномочий пользователя. По окончании срока хранения учетные записи удаляются из системы.

Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных работников, используя соответствующие ИС.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае руководителям СП Учреждения, в котором числится такой работник согласно штатному расписанию (для работников не входящих в штат Учреждения – руководителям СП курирующего соответствующие договорные отношения) вменяется в обязанность своевременно подавать заявки на блокирование учетной записи работника не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указывается:

– должность работника (с полным наименованием подразделения), фамилия, имя и отчество работника;

– имя пользователя (учетной записи) данного работника;

– дата прекращения полномочий пользователя.

Заявку подписывает руководитель Учреждения, в котором числится работник согласно штатному расписанию (для работников не входящих в штат Учреждения – руководитель СП, курирующего соответствующие договорные отношения), утверждая тем самым факт прекращения срока действия полномочий пользователя.

Администратор ИБ рассматривает представленную заявку и производит блокировку учетной записи пользователя. При отсутствии технической возможности действия по блокировке учетных записей пользователей производятся уполномоченными работниками сервисной организации под контролем администратора ИБ.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае производственной необходимости сохранения персональных документов (профайла пользователя) на АРМ работника после прекращения срока действия его полномочий руководитель СП Учреждения, в котором числился работник согласно штатному расписанию (для работников не входящих в штат Учреждения – руководитель СП курирующего соответствующие договорные отношения) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия полномочий пользователя) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных работников.

Такая заявка должна быть предварительно согласована с администратором ИБ.

11. Политика использования информационных ресурсов в рамках существующих информационных систем

Настоящая Политика определяет основные правила использования информационных ресурсов Учреждения в рамках существующих информационных систем. В процессе работы Учреждения могут вводиться новые дополнительные информационные ресурсы.

При создании нового информационного ресурса в составе Учреждения необходимо произвести следующие процедуры:

– назначить администратора нового информационного ресурса;

– сформировать заявку на создание нового информационного ресурса;

– составить список привилегированных пользователей настоящего информационного ресурса;

– составить список ролей (матрицу доступа) и описание (паспорт) ролей пользователей информационного ресурса с указанием разрешенных видов доступа к ресурсам.

Заявка на создание нового информационного ресурса должна включать:

– наименование созданного ресурса;

– наименование ИС, в рамках которой создается настоящий ресурс;

– назначение ресурса;

– класс (уровень конфиденциальности) ресурса;

– расположение ресурса.

Заявка формируется администратором настоящего информационного ресурса и передается администратору информационной безопасности для согласования.

Заявка подписывается администратором (владельцем) нового информационного ресурса и согласуется:

– администратором (владельцем) информационной системы, в рамках которой создается ресурс;

– администратором ИБ.

Передача Заявок осуществляется в соответствии с регламентом документооборота Учреждения. Оригинал Заявки передается администратору ИБ. В случае невозможности организации требуемого информационного ресурса, администратор ИБ должен направить администратору нового информационного ресурса мотивированный отказ в письменной форме с приложением Заявки.

Список пользователей, имеющих доступ к настоящему информационному ресурсу, формируется на основании «Политики предоставления доступа к информационному ресурсу», действующей в Учреждении.

12. Политика безопасности электронной почты

Настоящая Политика определяет основные правила безопасного использования электронной почты Учреждения.

Использование электронной почты должно производиться посредством служебных электронных почтовых адресов.

Использование электронной почты должно осуществляться только для выполнения функциональных обязанностей.

Информация ограниченного доступа, передаваемая с использованием электронной почты, должна быть защищена от несанкционированного просмотра или модификации.

Передача конфиденциальной информации средствами электронной почты запрещена.

Запрещается использование электронной почты, нарушающее нормы действующего законодательства, этики и корпоративной культуры, а также авторские и смежные права других лиц или представляющее собой любую форму преследования личности.

Факты отправки и приема сообщений электронной почты должны фиксироваться, а сообщения – сохраняться.

Перед отправкой сообщений электронной почты необходимо проверять правильность указания адресов получателей.

13. Политика безопасности использования интернет

Настоящая Политика определяет основные правила для безопасного использования Интернет работниками Учреждения.

Использование сети Интернет должно осуществляться только для выполнения функциональных обязанностей.

Информация ограниченного доступа и конфиденциальная информация, передаваемая по сетям общего доступа (сеть Интернет), должна быть защищена от несанкционированного просмотра или модификации. При этом средства защиты конфиденциальной информации должны быть сертифицированы.

Запрещается использование сети Интернет, нарушающее нормы действующего законодательства, этики и корпоративной культуры, а также авторские и смежные права других лиц.

Запрещается использование сети Интернет для публикации информации от имени Учреждения без соответствующей санкции руководства.

Содержание и объем информации, передаваемой или принимаемой с использованием сети Интернет, могут ограничиваться.

Учреждение оставляет за собой право мониторинга использования сети Интернет с целью соблюдения требований Политики.

14. Политика учетных записей

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов Учреждения.

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации / аутентификации пользователей информационных активов Учреждения;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Учреждения назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

15. Политика использования паролей

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к информационным активам Учреждения.

Идентификация / аутентификация пользователей осуществляется посредством использования смарт-карт или, при отсутствии технической возможности их использования, паролей.

Доступ к информационным активам Учреждения должен производиться с использованием персональных учетных записей и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

– пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;

– символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

– не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;

– не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.), не содержать легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т. п.);

– при смене пароля новое значение должно отличаться от предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам;

– смена паролей не более чем через 90 дней.

Временный пароль, создаваемый администратором при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем при первом обращении к активу.

Пароли, предустановленные производителем, должны сменяться до начала эксплуатации актива.

Пароли ключевых учетных записей критически важных информационных активов должны сохраняться в запечатанном конверте в сейфе руководителя подразделения – владельца соответствующего актива.

Запрещается:

– сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);

– сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

– использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -* F%2hTR8 -> F%3hTR8, или F%1hTR8 -* Fl%hTR8 -* F1h%TR8 и др.);

– использовать учетные записи других лиц;

– использовать вне Учреждения пароли, совпадающие с паролями доступа к его информационно-технологическим активам;

– использовать в качестве паролей примеры, приведенные в Политике.

Смена пароля должна производиться не реже одного раза в шесть месяцев или при обнаружении фактов, указывающих на его возможную компрометацию, а в отношении административных учетных записей – также при смене лица, выполняющего административные функции.

В зависимости от критичности информационно-технологического актива, его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

Процессы создания, изменения, использования, блокирования, удаления учетных записей, а также смены паролей должны регламентироваться, протоколироваться, и контролироваться.

16. Политика защиты АРМ

Настоящая Политика определяет основные правила и требования по защите конфиденциальной информации Учреждения от неавторизованного доступа, утраты или модификации.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр, не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

На АРМах работников СП должны выполняться требования к АРМ ИОГВ ВО и подведомственным им учреждений.

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Техническое обслуживание должно осуществляться только на основании обращения пользователя в отдел технической поддержки, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован, и контролируется.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей,

содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом системного администрирования, и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию – регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими работниками Учреждения. Запрещается использование указанных АРМ другими пользователями без согласования с администратором ИБ.

17. Порядок сопровождения ИС

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла.

ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (далее – ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации).

Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться. На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

– неверной формулировки требований к ИС;

– выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;

– принятия неверных проектных решений;

– внесения разработчиком дефектов на уровне архитектурных решений;

– внесения разработчиком недокументированных возможностей в ИС;

– неадекватной (неполной, противоречивой, некорректной и пр.) реализации

– требований к ИС;

– разработки некачественной документации;

– сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС, либо к неадекватной реализации требований;

– неверного конфигурирования ИС;

– приемки ИС, не отвечающей требованиям заказчика;

– внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Учреждения должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности бизнеса.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

– умышленное несанкционированное раскрытие, модификация или уничтожение информации

– неумышленная модификация или уничтожение информации;

– недоставка или ошибочная доставка информации;

– отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения.

На стадии сопровождения должна быть обеспечена защита от угроз:

– внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

– невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести

ущерб Учреждению, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

18. Ликвидация последствий и ответственность нарушителей правил ИБ

Ответственность за выполнение правил безопасности несет каждый работник Учреждения в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 ТК РФ работники, нарушающие требования политики безопасности Учреждения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все работники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил политики ИБ (ст. 238 ТК РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, работники Учреждения несут материальную ответственность в полном размере причиненного ущерба (ст. 243 ТК РФ).

За неправомерный доступ к охраняемой законом компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ (автоматизированной системы обработки информации), повлекшее уничтожение, блокирование или модификацию защищаемой информации, причинившее крупный ущерб, работники Учреждения несут ответственность в соответствии с уголовным законодательством Российской Федерации. Информация о выявлении подобного рода нарушений передается в правоохранительные органы.

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации Учреждения, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам Учреждения и предпринимать меры по их локализации и устранению.

ПРИЛОЖЕНИЯ

Приложение 1

Форма заявления на создание учетной записи пользователя

СОГЛАСОВАНО

Лицо, ответственное за ведение
кадрового делопроизводства

«___» _____ 20__г.

Администратор
информационной безопасности

«___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____

На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование структурного подразделения	
ФИО работника, должность, телефон	
ФИО непосредственного руководителя, должность, телефон	

Работник приступает к работе с: «___» _____ 20__г. по «___» _____ 20__г.
(указывается при необходимости)

Обоснование служебной
необходимости:_____

_____

Руководитель структурного подразделения _____
(наименование подразделения)

_____ _____ «___» _____ 20__г.
(Ф.И.О. руководителя подразделения) (подпись) (дата)

С правилами работы в информационной системе КУ ВО «ГАОПИ ВО» и указанными службами ознакомлен:

_____ _____ «___» _____ 20__г.
(Ф.И.О. работника) (подпись) (дата)

Выполнено:_____ _____
(назначенное имя пользователя) (адрес корпоративной почты)

Администратор информационной безопасности _____ _____
(Фамилия И.О.) (Подпись)

Дата: «___» _____ 20__г.

Приложение 2

Форма заявления на изменение полномочий

СОГЛАСОВАНО

Владелец информационного актива «___» _____ 20__г.

Владелец информационного актива
(при совместном владении
информационным активом)

«___» _____ 20__г.

Администратор информационной безопасности

«___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____
На изменение полномочий пользователю

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование структурного подразделения	
ФИО работника, должность, телефон	
Имя в системе (указывается если есть)	
ФИО непосредственного руководителя, должность, телефон	
Наименование информационного ресурса	
Старые полномочия (если были)	
Новые полномочия	

Изменения вступают в силу с: «___»_____ 20__г. по «___» _____ 20__г.
(указывается при необходимости)

Обоснование служебной необходимости: _____

_____

Руководитель структурного подразделения _____
(наименование подразделения)

_____ _____ «___» _____ 20__г.
(Ф.И.О. руководителя подразделения) (подпись) (дата)

С правилами работы в информационной системе КУ ВО «ГАОПИ ВО» и указанными службами ознакомлен:

_____ _____ «___» _____ 20__г.
(Ф.И.О. работника) (подпись) (дата)

Выполнено:_____ _____
(назначенное имя пользователя) (адрес корпоративной почты)

Администратор информационной безопасности _____ _____
(Фамилия И.О.) (Подпись)

Дата: «___» _____ 20__г.

Приложение 3

Форма заявления на блокировку учетной записи

ЗАЯВЛЕНИЕ № _____
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование структурного подразделения	
ФИО работника, должность, телефон	
ФИО непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: «___» _____ 20__г.

Обоснование блокировки:_____

_____

_____

Руководитель структурного подразделения _____
(наименование подразделения)

_____ _____ «___» _____ 20__г.
(Ф.И.О. руководителя подразделения) (Подпись) (дата)

С гарантированным хранением данных в течении
_____
(указывается срок хранения данных пользователя)

Пользователь блокирован

Системное Время: ____чч____мм
Администратор информационной безопасности _____ _____
(Фамилия И.О.) (Подпись)

Дата: «___» _____ 20__г.

Приложение 4

Форма заявления на создание нового информационного ресурса в рамках действующей ИС

СОГЛАСОВАНО

Владелец информационного актива «___» _____ 20__г.

Владелец информационного актива
(при совместном владении информационным активом)

«___» _____ 20__г.

Администратор информационной безопасности

«___» _____ 20__г.

ЗАЯВЛЕНИЕ № _____

На создание нового информационного ресурса

Прошу создать новый информационный ресурс:

Наименование информационного ресурса	
Наименование ИС, в рамках которой создается информационный ресурс	
Назначение информационного ресурса	
Категория конфиденциальности	
ФИО, должность, телефон ответственного (владельца) информационного ресурса	
ФИО, должность, уровень полномочий привилегированных пользователей информационного ресурса	

Обоснование служебной необходимости: _____
_____

Ответственный (владелец) информационного ресурса _____
_____
(наименование подразделения)

_____ _____ «___» _____ 20__г.
(Ф.И.О. руководителя подразделения) (Подпись) (дата)

Выполнено:_____
_____
_____
(системное имя информационного ресурса, описание выполненных действий)

Системное Время: ____чч____мм

Администратор информационной безопасности _____ _____
(Фамилия И.О.) (Подпись)

Дата: «___» _____ 20__г.

Приложение 2
к приказу № 20 – О
от «20» июля 2022

ИНСТРУКЦИЯ
администратора информационной безопасности объектов информатизации казенного учреждения Воронежской области «Государственный архив общественно-политической истории Воронежской области»

1. Общие положения

Настоящая Инструкция определяет функции, права и обязанности администратора информационной безопасности объектов информатизации (далее – ОИ) казенного учреждения Воронежской области «Государственный архив общественно-политической истории Воронежской области» (далее – Учреждение) по вопросам обеспечения информационной безопасности при обработке информации ограниченного доступа.

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима защиты информации ограниченного доступа и является обязательной к исполнению в КУ ВО «ГАОПИ ВО».

2. Основные функции администратора информационной безопасности

Основными функциями администратора информационной безопасности объектов информатизации (далее – Администратор) являются:

2.1. Руководство и контроль планирования и выполнения организационных мероприятий по вопросам организации безопасности информации (ОБИ) в Учреждении.

2.2. Ведение, а также актуализация документов по обеспечению безопасности информации ограниченного доступа, в том числе:

– приказов по вопросам ОБИ;

– частных моделей угроз безопасности информационных систем;

– положений, руководств, регламентов и инструкций по вопросам организации и контроля ОБИ;

– технических паспортов ОИ;

– списков пользователей ОИ с указанием прав доступа (по подразделениям и ИС);

– документацию на средства защиты информации (СрЗИ), в том числе на средства криптографической (шифровальной) защиты информации, включая лицензии, сертификаты;

– документы, подтверждающие соответствие ОИ требованиям безопасности;

– перечни защищаемых информационных ресурсов и работников, допущенных к работе с этими ресурсами;

– перечни помещений, в которых осуществляется обработка информации ограниченного доступа;

– журналы учета, хранения и эксплуатации средств защиты информации, носителей ПДн;

– схемы расположения СрЗИ относительно границ контролируемых зон.

2.3. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты информации ограниченного доступа, при проведении работ на ОИ и в информационных системах (ИС).

2.4. Администратор является ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации (при принятии решения использования таких средств в Учреждении) и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

2.5. Контроль за периодическим проведением смены паролей для доступа к СЗИ пользователями.

2.6. Учет машинных носителей информации, используемых в ИС ОИ для хранения и обработки информации ограниченного доступа.

2.7. Регламентация и контроль использования технологий беспроводного доступа: ведение мониторинга и проведения периодического контроля применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа ИС.

2.8. Регламентация и контроль использования в информационной системе мобильных технических устройств: организация мониторинга и периодического контроля применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

2.9. Организация проведения мероприятий по обеспечению антивирусной защиты: проведение периодического тестирования средствами антивирусной защиты компонентов ОИ (АРМ и серверов) на наличие вредоносных компьютерных программ.

2.10. Проведение периодического контроля состава технических средств, программного обеспечения и средств защиты информации, применяемых в ИС ОИ.

2.11. Контроль за размещением устройств вывода (отображения) информации.

2.12. Определение перечня лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

2.13. Совместно с ответственными за ОБИ в ИС осуществляет учет физического доступа к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

2.14. Сопровождение СЗИ:

– проведение контроля целостности аппаратно-программной среды средств защиты информации (далее – СрЗИ) в необходимое значение;

– периодическое тестирование СрЗИ, установленных на ОИ, входящих в СЗИ, особенно при изменении программной среды и полномочий исполнителей;

– проведение контроля установки обновлений программного обеспечения, включая программное обеспечение СрЗИ не реже 1 раза в год с фиксацией в соответствующих журналах;

– восстановление программной среды, программных средств и настроек СрЗИ при сбоях;

– поддержание установленного порядка и правил антивирусной защиты информации на ОИ, входящих в состав СЗИ;

2.15. Хранение документации на ОИ, входящих в состав СЗИ, контроль ее соответствия реальным конфигурациям данных и учет изменений программной конфигурации;

2.16. Проведение инструктажа работников Учреждения (пользователей ИС) по правилам работы с используемыми СрЗИ и обеспечению безопасности обрабатываемой информации ограниченного доступа.

2.17. Организация проведения мероприятий по обеспечению и контролю защиты информации в среде виртуализации, в том числе внутри виртуальных машин, а также управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

3. Права Администратора

Администратор имеет право:

– требовать от пользователей ОИ соблюдения установленных технологий обработки информации и выполнения правил пользования объектами информатизации, определяющих политику информационной безопасности, в том числе в отношении обработки персональных данных и доступа к государственным информационным системам;

– участвовать в анализе ситуаций, касающихся функционирования СрЗИ и расследования фактов несанкционированного доступа;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4. Обязанности Администратора:

Администратор обязан:

– обеспечивать функционирование и поддерживать работоспособность СрЗИ в пределах возложенных функций;

– проводить инструктаж пользователей по правилам работы в ИС ОИ;

– осуществлять плановые и внеплановые проверки по выполнению работниками Учреждения требований по защите информации;

– в случае отказа СрЗИ принимать меры по их восстановлению;

– докладывать руководству о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

– вести документацию на СЗИ в соответствии с требованиями нормативных документов.

Приложение 3
к приказу № 20 – О
от «20» июля 2022

ИНСТРУКЦИЯ
пользователя при работе на автоматизированном рабочем месте казенного учреждения Воронежской области «Государственный архив общественно-политической истории Воронежской области»

1. Обязанности пользователя автоматизированного рабочего места

Пользователь автоматизированного рабочего места (далее – Пользователь) обязан:

– перед началом работы на автоматизированном рабочем месте (далее – АРМ) визуально осмотреть технические средства на наличие физических повреждений, целостности пломб (при наличии);

– знать и соблюдать установленные требования настоящей Инструкции;

– соблюдать требования парольной защиты (раздел 3 настоящей Инструкции);

– соблюдать правила антивирусной защиты (раздел 2 настоящей Инструкции);

– соблюдать правила при работе в сети Интернет (раздел 5 настоящей Инструкции);

– соблюдать правила при работе с электронной почтой (раздел 4 настоящей Инструкции);

- знать состав и правила пользования программно-аппаратными средствами обеспечения безопасности информации согласно документации на них;

– во время работы следить за тем, чтобы посторонние лица не могли прочесть информацию, выводимую на экран дисплея;

– сообщать администратору информационной безопасности о нарушениях обеспечения безопасности информации и фактах несанкционированного доступа к информации и техническим средствам объекта. При возникновение нештатных ситуаций в работе пользователь обязан приостановить работу и сообщить об этом Администратору информационной безопасности (в соответствии с политикой безопасности Учреждения).

– сообщать администратору информационной безопасности об отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

– сообщать администратору информационной безопасности о некорректном функционировании установленных на компьютеры технических средств защиты.

Пользователю запрещается:

- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.
- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства;

– выполнять операции, не предусмотренные технологическим процессом обработки информации на объекте, использовать при работе неучтенные носители информации и средства, не входящие в состав АРМ;

- записывать и хранить на неучтенных машинных носителях информации;

– оставлять незаблокированным АРМ при отсутствии на рабочем месте;

– подключать к рабочей станции и корпоративной информационной сети (ЕИТКС правительства Воронежской области) личные внешние носители и мобильные устройства;

– вносить изменения в состав программного обеспечения АРМ.

2. Правила антивирусной защиты

К использованию на компьютерах допускаются только лицензионные антивирусные средства.

Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором информационной безопасности.

Администратор информационной безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности.

Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям.

Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить

непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов.

3. Правила парольной защиты

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

– пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;

– символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

– не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;

– не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.), не содержать легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам.

4. Правила по работе с электронной почтой

При использовании электронной почты запрещено:

- использовать электронную почту в личных целях;
- передача конфиденциальной информации средствами электронной почты;
- использование электронной почты, нарушающее нормы действующего законодательства, этики и корпоративной культуры, а также авторские и смежные права других лиц или представляющее собой любую форму преследования личности;
- переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей;
- по собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений (если рассылка не связана с выполнением служебных обязанностей).

5. Правило по работе в сети Интернет

При доступе в Интернет пользователи обязаны соблюдать следующие правила:

- получать и отправлять по каналам сети Интернет только информацию, которая не противоречит законодательству Российской Федерации, а также международному законодательству;
- не использовать сеть Интернет для распространения получателю не запрошенной информации (создания или участия в сетевом шуме – спаме);
- не использовать идентификационные данные (имена, адреса, телефоны и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);
- не фальсифицировать свой IP-адрес, адреса, используемые в других сетевых протоколах, а также прочую служебную информацию при передаче данных в сети Интернет;
- не использовать сеть Интернет для приема, передачи и записи файлов мультимедиа (видео, музыка, игры, графика), а также стороннего программного обеспечения, не связанных с выполнением непосредственных служебных обязанностей пользователя.

При работе с ресурсами Интернета запрещается:

- использовать ресурсы сети Интернет в личных целях;
- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- самостоятельно загружать, устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- использовать анонимные прокси-серверы.

Приложение 4
к приказу № 20 – О
от «20» июля 2022

ИНСТРУКЦИЯ
пользователя объекта информатизации казенного учреждения Воронежской области «Государственный архив общественно-политической истории Воронежской области»

1. Общие положения

1.1. Объект информатизации (далее – ОИ) казенного учреждения Воронежской области «Государственный архив общественно-политической истории Воронежской области» (далее – Учреждение) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров (ГОСТ Р.51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию).

Пользователь ОИ, на которых ведется обработка информации ограниченного доступа не составляющая государственную тайну (далее – Пользователь), осуществляет обработку информации ограниченного доступа, в том числе в информационных системах (далее – ИС) ОИ.

При обработке служебной информации ограниченного распространения в Учреждении следует также руководствоваться инструкцией о порядке обращения со служебной информацией ограниченного распространения в исполнительных органах государственной власти Воронежской области, утвержденной постановлением правительства Воронежской области от 11.08.2015 № 667.

1.2. Пользователи ОИ имеют разные права доступа к информации, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.

1.3. В процессе работы Пользователь ОИ несет персональную ответственность за обеспечение безопасности информации.

1.4. Хранение и обработка информации на ОИ разрешается только на учтенных носителях информации.

2. Правила допуска пользователей к работе на объекте информатизации

2.1. Допуск пользователей для работы на ОИ осуществляется в соответствии со списком лиц, утвержденным руководителем Учреждения.

2.2. Учет работы пользователей на ОИ производится, в том числе, использованием средств защиты информации от несанкционированного доступа (СЗИ от НСД), установленных на ОИ, в системном журнале средств защиты информации.

2.3. Запрещается нахождение в помещениях, где ведется обработка информации ограниченного доступа, посторонних лиц, не имеющих полномочий по доступу к информации ограниченного доступа, без нахождения в помещении ответственного работника (или работника, постоянно допущенного к работе в помещении).

В рабочее время, в случае ухода всех работников, или в нерабочее время помещения, где производится обработка информации ограниченного доступа, должны закрываться на ключ.

Должны выполняться все предписания на эксплуатацию средств защиты информации, связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении, где происходит обработка информации ограниченного доступа.

Уборка помещений должна производиться под контролем работника, имеющего доступ в помещение и постоянно в нем работающего.

Выносить технические средства обработки информации ограниченного доступа за пределы контролируемой зоны учреждения с целью их ремонта, замены и т. п. без согласования с ответственным за обеспечение информационной безопасности. При принятии решения о выносе компьютеров жесткие магнитные диски должны быть демонтированы и сданы на хранение администратору информационной безопасности.

Мониторы технических средств обработки информации ограниченного доступа должны быть размещены таким образом, чтобы исключалась возможность случайного или преднамеренного визуального просмотра отображаемой на них информации посторонними лицами.

3. Обязанности Пользователя

3.1. Пользователь обязан:

- перед началом работы с ОИ визуально осмотреть технические средства на наличие физических повреждений, целостности пломб (при наличии);
- знать и соблюдать установленные требования настоящей Инструкции;
- соблюдать требования парольной защиты (пункт 6 настоящей Инструкции);
- соблюдать правила антивирусной защиты (пункт 4 настоящей Инструкции);
- соблюдать правила при работе в сети Интернет пункт 5 настоящей Инструкции);

- знать состав и правила пользования программно-аппаратными средствами обеспечения безопасности информации согласно документации на них;

– во время работы следить за тем, чтобы посторонние лица не могли прочесть информацию, выводимую на экран дисплея;

– сообщать администратору безопасности о нарушениях обеспечения безопасности информации и фактах несанкционированного доступа к информации и техническим средствам объекта. При возникновение нештатных ситуаций в работе ОИ пользователь обязан приостановить работу и сообщить об этом администратору информационной безопасности.

3.2. Пользователю запрещается:

- самостоятельно вносить изменения в состав программного обеспечения ОИ;

- выполнять операции, не предусмотренные технологическим процессом обработки информации на объекте, использовать при работе неучтенные носители информации и средства, не входящие в состав ОИ

- производить копирование персональных данных на неучтенные носители;

- оставлять незаблокированным ОИ при отсутствии на рабочем месте;

- выносить за пределы Учреждения или передавать третьим лицам персональные данные без согласования со своим руководителем и с администратором информационной безопасности;

– сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ОИ;

– подключать к рабочей станции и корпоративной информационной сети (ЕИТКС правительства Воронежской области) личные внешние носители и мобильные устройства;

– вносить изменения в состав программного обеспечения ОИ.

4. Организация антивирусной защиты

4.1. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая Пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию Пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте нештатной работы ОИ начальника своего отдела, администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– немедленно поставить в известность о факте обнаружения заражения вирусом файлов начальника своего отдела, администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с администратором информационной безопасности провести анализ возможности дальнейшего использования ОИ.

5. Правила доступа в Интернет и использования электронной почты

5.1. Пользователи ОИ при подключении к сети Интернет имеют право:

- использовать в работе предоставленные им ресурсы сети Интернет в оговоренных в настоящей инструкции рамках. Администратор информационной безопасности в праве организовать ограничение доступа к некоторым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;

- обращаться к администратору информационной безопасности по вопросам, связанным с распределением ресурсов компьютера;

– обращаться за помощью к администратору информационной безопасности при решении задач использования ресурсов сети Интернет;

- вносить предложения по улучшению работы с ресурсами сети Интернет.

5.2. Пользователю запрещается:

- самостоятельно загружать, устанавливать на ОИ прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

- использовать ресурсы сети Интернет на ОИ в не служебных целях;

- допускать к работе ОИ посторонних лиц;

- использовать для служебной переписки почтовые сервисы кроме govvrn.ru и yandex.ru;

– выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения);

- осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет;

- строго запрещается проводить подключение ОИ к ресурсам сети Интернет, через не служебный канал доступа – сотовый телефон, модем, и другие устройства.

5.3. Правила безопасного использования электронной почты:

- запрещается открывать почтовые вложения, попавшие Пользователю «по ошибке» (например, запрещается открывать присланное резюме, если пользователь не работает в кадровом подразделении Учреждения);

- при получении почтового вложения всегда необходимо уточнять у отправителя (по средствам телефонного звонка) в действительности отправки им сообщения, не открывая при этом никакие вложенные файлы и не переходя ни по каким ссылкам;

- запрещается открывать сообщения от своих коллег (знакомых) с просьбой открыть «не открывающийся файл, присланный ему по почте». В данном случае нужно незамедлительно обратиться к ответственному за обеспечение безопасности информации;

- запрещается публиковать адреса работников Учреждения на общедоступных интернет-ресурсах (форумы, конференции и т. п.) без предварительного согласования с ответственным за обеспечение безопасности информации;

– запрещается отправлять файлы, содержащие персональные данные по электронной почте;

– запрещается запуск исполняемых файлов из почтовой программы (с расширениями js, exe, vbs, cmd, scr, com, pif, wsf, bat, lnk и т.д.);

– апрещается открывать вложения из почтовой программы. Перед просмотром вложенного файла, его необходимо сохранить на жесткий диск ОИ и проверить антивирусной программой.

6. Порядок парольной защиты

6.1. Применяемые в Учреждении пароли (для учетных записей пользователей, удаленного доступа, для доступа к сетевому и коммутационному оборудованию, для управления средствами защиты информации и т.д.) должны удовлетворять следующим минимальным требованиям:

– пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;

– символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

– не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;

– не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.), не содержать легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т. п.);

– при смене пароля новое значение должно отличаться от предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам;

– смена паролей не более чем через 90 дней.

6.2. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

Запрещается:

- сообщать или разглашать свой пароль, включая коллег, работников службы технической поддержки (при наличии), любыми средствами и способами;
- хранить пароли на бумажном носителе, прикрепленном к монитору или лежащем на столе под клавиатурой, а также в других легко доступных для обнаружения местах, хранить пароли в текстовом документе на рабочем столе, хранить пароли для доступа к портальным информационным системам в браузере;
- использовать автоматическое сохранение пароля при входе в ИС;
- использовать одинаковые пароли в различных ИС;
- пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя;
- все текущие операции с паролем пользователь должен осуществлять лично, не допуская возможности рассмотреть состав вводимого пароля и порядок введения символов.
- пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей не принадлежащих им учетных записей.

7. Порядок работы со средствами защиты информации

7.1. Требования предъявляемые к средствам защиты информации.

7.1.1. Средства защиты информации (далее – СрЗИ) входящие в состав системы защиты информации Учреждения, эксплуатационная и техническая документация к ним, подлежат поэкземплярному учету.

7.1.2. Поэкземплярный учет СрЗИ ведет администратор информационной безопасности в журнале поэкземплярного учета СрЗИ, эксплуатационной и технической документации к ним. При этом программные СрЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СрЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие

СрЗИ учитываются также совместно с соответствующими аппаратными средствами.

7.1.3. Дистрибутивы СрЗИ на носителях, эксплуатационная и техническая документация к СрЗИ, инструкции хранятся у администратора информационной безопасности. Хранение осуществляется в закрываемых на замок хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.1.4. Аппаратные средства, с которыми осуществляется штатное функционирование СрЗИ, а также аппаратные и аппаратно-программные СрЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования), аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

7.1.5. К эксплуатации СрЗИ допускаются лица, изучившие документацию на данные СрЗИ (руководство пользователя).

7.1.6. Пользователям запрещается полное или частичное воспроизведение, тиражирование и распространение оптических носителей, содержащих дистрибутивы СрЗИ, а также лицензионный ключ СрЗИ.

7.2. Требования, предъявляемые к средствам криптографической защиты информации.

7.2.1. Средства криптографической защиты информации (далее – СКЗИ), эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

7.2.2. Поэкземплярный учет СКЗИ ведет Ответственный пользователь СКЗИ в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

7.2.3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

7.2.4. Ответственный пользователь СКЗИ заводит и ведет на каждого пользователя СКЗИ Лицевой счет, в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

7.2.5. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия)

непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией.

7.2.6. Ответственный пользователь СКЗИ заводит и ведет Журнал учета лиц, допущенных к работе с криптосредствами.

7.2.7. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей должны быть выданы под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

7.2.8. Дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к СКЗИ хранятся у Ответственного пользователя СКЗИ. Криптографические ключи на отчуждаемых носителях хранятся у Пользователей СКЗИ. Хранение осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.2.9. Пользователи СКЗИ могут осуществлять хранение рабочих и резервных криптографических ключей, предназначенных для применения в случае неработоспособности рабочих криптографических ключей. Резервные криптографические ключи могут также находится на хранении у Ответственного пользователя СКЗИ.

7.2.10. На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель – «Рабочий»; на другой ключевой носитель – «Резервный». Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается Пользователем СКЗИ и Ответственным пользователем СКЗИ.

7.2.11. Полученные рабочие и резервные криптографические ключи Ответственный пользователь СКЗИ обязан учесть в Лицевом счете Пользователя СКЗИ. Резервные криптографические ключи могут находиться на хранении у Ответственного пользователя СКЗИ.

7.2.12. Ключевые носители с неработоспособными криптографическими ключами Ответственный пользователь СКЗИ принимает от Пользователя СКЗИ под роспись в Лицевом счете Пользователя СКЗИ и в Журнале поэкземплярного учета. Неработоспособные ключевые носители подлежат уничтожению.

7.2.13. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ,

аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

7.2.14. Ключевые носители совместно с Техническим (аппаратным) журналом должны храниться Ответственным пользователем СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Аппаратный журнал совместно с другими документами, при этом ключевые носители и Аппаратный журнал должны быть помещены в отдельную папку.

7.3. Порядок обращения со СКЗИ.

7.3.1. Монтаж и установка СКЗИ осуществляется уполномоченным лицом – Ответственным пользователем СКЗИ.

7.3.2. Пользователь СКЗИ обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

7.3.3. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной пользователю по роду выполняемых функциональных обязанностей.

7.3.4. Пользователь обязан немедленно уведомлять Ответственного пользователя СКЗИ о случаях компрометации криптографических ключей.

7.3.5. Допуск пользователей к работе со СКЗИ осуществляется на основании приказа руководителя Учреждения.

7.3.6. Пользователь СКЗИ перед началом работы со СКЗИ должен быть ознакомлен под роспись с приказом ФАПСИ России от 13.06.2001 № 152 «Об утверждении Инструкции об организации обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведения, составляющих государственную тайну».

8. Ответственность Пользователя

8.1. Пользователь несет персональную ответственность за соблюдение установленных требований во время работы на ОИ.

8.2. Пользователи, виновные в нарушении настоящей инструкции и законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение 5
к приказу № 20 – О
от «20» июля 2022

ИНСТРУКЦИЯ
пользователя КУ ВО «Государственный архив общественно-политической истории Воронежской области» в части обеспечения безопасности информации при ее обработке в государственных информационных системах

1. Общие требования по обеспечению безопасности обработки информации в государственных информационных системах

1.1. Ответственность за организацию защиты информации в государственных информационных системах (далее – ГИС) и выполнение установленных условий ее функционирования возлагается на ответственного за обеспечение безопасности в государственных информационных системах. Ответственность за выполнение мероприятий по обеспечению безопасности информации возлагается на лицо, производящее ее обработку (пользователя ГИС).

1.2. Допуск пользователей к работе в ГИС осуществляет оператор ГИС в соответствии с установленными правилами.

1.3. К самостоятельной работе на объектах информатизации (далее – ОИ), входящих в состав ГИС, допускаются лица, изучившие требования настоящей Инструкции, освоившие правила эксплуатации ОИ и изучившие инструкцию пользователя ОИ для обработки информации ограниченного доступа.

Проверку знаний пользователями настоящей Инструкции и практических навыков в работе осуществляет администратор безопасности ГИС.

2. Обязанности пользователя ГИС

2.1. При первичном допуске к работе в ГИС, пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию.

2.2. Каждый пользователь ГИС, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации ограниченного доступа и имеющий доступ к аппаратным средствам, программному обеспечению и данным ГИС, несет персональную

ответственность за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ГИС.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ГИС.

2.2.3. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.4. Немедленно ставить в известность администратора безопасности ГИС:

- при подозрении компрометации личного пароля;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ГИС;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ГИС, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов и попыток несанкционированного доступа к и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения в ГИС.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ГИС или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации ограниченного доступа в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информации ограниченного доступа на неучтенных носителях информации.

2.3.5. Оставлять без личного присмотра на ОИ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информации ограниченного доступа.

2.3.6. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц.

2.3.7. Производить перемещения технических средств ОИ без согласования с ответственным за обеспечение защиты информации в ГИС

ДСМК ВО и ответственным за обеспечение безопасности информации ограниченного доступа.

2.3.8. Подключать к ОИ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.9. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.10. Оставлять без контроля ОИ в процессе обработки информации ограниченного доступа.

2.3.11. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств ОИ.

Приложение 6
к приказу № 20 – О
от «20» июля 2022

ИНСТРУКЦИЯ
КУ ВО «Государственный архив общественно-политической истории Воронежской области» по обеспечению безопасности использования квалифицированной подписи и средств квалифицированной электронной подписи

1. Общие положения

Настоящая инструкция составлена в соответствии с требованиями Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

– Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, в части обращения со средствами криптографической защиты информации;

– Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66, в части эксплуатации средств криптографической защиты информации;

– эксплуатационной документации к средствам электронной подписи;

– приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

– должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

– внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Использовать пароли в соответствии со следующими правилами:

– пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;

– символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

– не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;

– не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.), не содержать легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т. п.);

– при смене пароля новое значение должно отличаться от предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам;

– смена паролей не более чем через 90 дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

– не использовать нестандартные, измененные или отладочные версии операционных систем;

– исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

– на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

– все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень; – всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

– необходимо предусмотреть меры, максимально ограничивающие доступ к следующему: системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации (пароли и т.п.), отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

– организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

– исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий; – регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.1.5. Необходимо организовать и использовать:

– систему аудита, организовать регулярный анализ результатов аудита;

– комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

– осуществлять несанкционированное копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;

– использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

– удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи. Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

– на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;

– должно быть установлено только лицензионное программное обеспечение;

– должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных; – должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

– должны регулярно устанавливаться обновления операционной системы;

– должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц,

не имеющих полномочий для работы в соответствующей информационной системе;

– должна быть активирована регистрация событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного работника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.