Приложение №2 к Приказу от 02 мая 2023 №59-ОД

Бюджетное государственное учреждение Ивановской области
«Ивановская областная ветеринарная лаборатория»

Методическое пособие по защите информации

Термин "информационная безопасность" может иметь различный смысл и трактовку в зависимости от контекста. В общем смысле под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", определяет понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

— **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

— **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

— **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

— по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;

— по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

— по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

— по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

1) законодательный – законы и подзаконные нормативные акты Российской Федерации;

2) административный – комплекс мер, предпринимаемых локально руководством организации;

3) процедурный уровень – меры безопасности, реализуемые людьми;

4) программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

В сфере информационной безопасности существуют следующие органы, регулирующие ее:

Федеральная служба безопасности Российской Федерации (ФСБ России). Обеспечивает безопасность в стране в пределах своих полномочий: например, сертифицирует средства защиты информации.

Федеральная служба охраны Российской Федерации (ФСО России). Разрабатывает и реализует государственную политику и правовые акты в сфере охраны сведений, которые относятся к государственной власти, обеспечивает спецсвязь между органами государственной власти.

Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК). Реализует и поддерживает политику государства в сфере информационной безопасности, осуществляет взаимодействие между другими ведомствами.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (Роскомнадзор). Контролирует деятельность средств массовой информации по предоставлению недостоверной информации или утечке сведений, составляющих государственную тайну. Исполняет функции надзора за соблюдением требований к системам, обрабатывающим персональные данные граждан.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь). Разрабатывает и реализует Государственную политику и нормативно-правовую документацию в сфере информационных технологий, Средств массовой информации, электросвязи и т. д.

Соблюдение следующих федеральных законов обязательно для сохранения безопасности информации при работе с ней:

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

Ключевые моменты закона об информационной безопасности:

— Нельзя собирать и распространять информацию о жизни человека без его согласия.

— Все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

— Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

— У государства есть реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории России.

— Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор — тогда его сайт разблокируют.

Руководящие приказы и положения по реализации мероприятий по обеспечению безопасности информации:

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Приказ Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 14.03.2014 №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, предоставляющих повышенную опасность для жизни и здоровья людей и для окружающих природной среды»;

Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а также иные нормативные правовые акты ФСТЭК России, ФСБ России.

Общие рекомендации к защите информации

Сотрудник(-и), уполномоченные руководителем органа для решения задач в сфере защиты информации, должны обладать как минимум навыками

работы как с программными так и аппаратно-программными средствами защиты информации. Оптимальным решением при назначении сотрудника на должность (поручения к исполнению обязанностей по защите информации) является переподготовка или повышение квалификации по программам защиты информации в образовательных организациях или учреждениях, осуществляющих подготовку специалистов в области информационной безопасности по программам, согласованным с ФСТЭК России. Приказ Министерства образования и науки РФ №1316 от 19.10.2020 года устанавливает срок освоения программ профессиональной переподготовки в области информационной безопасности – не менее 360 часов. Перечень организаций, осуществляющих образовательную деятельность по вопросам защиты информации, приведен на официальном сайте ФСТЭК – fstec.ru/Техническая защита информации/Обучение специалистов/Перечень организаций, осуществляющих образовательную деятельность.

Рекомендуются к использованию только сертифицированные серийно выпускаемые в защищённом исполнении технические средства обработки, передачи и хранения информации.

Используемые сертифицированные средства должны удовлетворять стандартам по электромагнитной совместимости, соответствующим уровню конфиденциальности информации.

Размещение объектов защиты должно быть в пределах контролируемой зоны (КЗ - территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств без постоянного или разового допуска).

Должна быть организована физическая защита помещений и самих технических средств с помощью сил охраны и иных технических средств (например ключ доступа, пароль или иные), предотвращающих или существенно затрудняющих проникновение в здания/помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри КЗ технических средств разведки или промышленного шпионажа.

Требования к рабочему месту

На рабочей станции (персональный компьютер) должно быть уставлено программное обеспечение (ПО) или программно-аппаратное решение для защиты информации, разграничения, защиты и контроля доступа, межсетевого экранирования и доверенной загрузки (средства защиты информации) к примеру DALLAS LOCK, Secret Net.

Рабочая станция должна быть оборудована антивирусной программой (специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления заражённых такими программами файлов и профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом), например Kaspersky, Dr.Web или

иной антивирусной программой (в средне-срочной перспективе должно быть принято во внимание положение п.6 Указа Президента Российской Федерации от 01 мая 2022 года № 250). Используемые в организации(предприятии) антивирусные средства должны быть лицензионными, а при необходимости иметь сертификат соответствия ФСТЭК и ФСБ России. Антивирусное средство должно на регулярной основе получать обновления антивирусных баз.

На рабочей станции администратором должен быть установлен сложный пароль (состоящий минимум из 6 символов, включающий в себя большие и маленькие буквы, цифры и специальные символы - например «!», «*» и т.д.). Не следует составлять пароль из личных данных, таких как имя, фамилия, прозвище, важные даты, ИНН, СНИЛС, номера телефона, возраста или адреса и очевидных фраз, слов или наборов символов. Пароль не может храниться в открытом виде на (под) клавиатуре, мониторе, столе или ящике стола. Смена пароля осуществляется не реже чем раз в 180 дней, в зависимости от установленного уровня защищенности. Не допускается передача данных и паролей третьим лицам, во избежание утечки информации и передачи ее злоумышленникам.

Рабочее место (персональный компьютер) должно функционировать под управлением лицензионной операционной системой (Windows, LINUX или иной), получающей на регулярной основе обновления безопасности.

Размещение устройств вывода (отображения) информации (монитор), должно исключать несанкционированный просмотр информации посторонними лицами.

Не допускается оставление рабочего места (персонального компьютера) включённым во время отсутствия сотрудника. При необходимости отлучиться с рабочего места, должен быть задействован механизм блокирования персонального компьютера (невозможность постороннего лица получить к нему доступ для получения любого вида информации).

Требования к механизмам получения-обработки информации

Не рекомендуется хранить учетные данные для доступа к ресурсам сети «Интернет» в web-браузере или в отдельных файлах, хранящихся на персональном компьютере.

Рекомендуется:

- регулярно отслеживать работоспособность антивирусных средств и межсетевых экранов, конфигурацию их настройки, а также актуальность баз данных компьютерных вирусов;

- проверять антивирусными средствами полученные файлы из сети «Интернет», в том числе по электронной почте. Не рекомендуется открывать электронные письма от неизвестных пользователей;

- использовать для работы с электронной почтой клиенты, работающие с использованием защищенного протокола обмена данными;

- осуществлять настройку web-браузеров для блокировки выполнения сценариев и другого потенциально опасного контента (Java-апплетов, Flash, ActiveX, Node.js и т.п.);

- своевременно обновлять операционные системы и программное обеспечение, а также регулярно проводить резервное копирование информации, хранящейся на персональном компьютере.

Требования к защите информации при межсетевом взаимодействии

Взаимодействие локально вычислительной сети (ЛВС) с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

При конфигурировании коммуникационного оборудования и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагмента на производственной основе и видам деятельности предприятия.

Подключение ЛВС к другой автоматизированной системы (АС) иного класса защищенности должно осуществляться с использованием межсетевого экрана (МЭ), требования к которому определяются Руководящим документом Государственной технической комиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» с помощью специализированных программ, одобренных ФСТЭКом.

Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты (например VipNet, КриптоПро и т.д.).