ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГРАМОТНОСТЬ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В современных условиях внедрения информационно-коммуникационных технологий во все сферы жизни общества и государства, цифровизации различных областей социального пространства особую актуальность приобретает сохранение в целостности, а зачастую и в тайне, информации служебного характера. Соответственно необходимость обеспечения информационной безопасности (далее – ИБ) в повседневной деятельности сотрудников органов внутренних дел (далее – ОВД) обусловлена наличием целого ряда взаимосвязанных факторов, большинство из которых являются следствием названного процесса информатизации и становления информационного общества. Качественно улучшенная эффективность информационного обеспечения деятельности в ОВД предопределила и отдельные проблемы обеспечения ведомственной ИБ.

В последние годы в связи с внедрением в деятельность ОВД современных информационных систем (далее – ИС), предназначенных для обработки и хранения информации, созданием единой цифровой платформы, изменением геополитической ситуации вокруг Республики Беларусь, обеспечение ИБ ОВД приобрело особую актуальность и значимость. Формирование интегрированных банков данных оперативно-служебной информации с организацией быстрого доступа к ним сотрудников непосредственно с рабочих мест, создание локальных вычислительных сетей в службах и подразделениях ОВД существенно обострили проблему защиты компьютерной информации ограниченного распространения. Это предопределяет необходимость формирования знаний, умений и навыков обеспечения ИБ.

В целом под ИБ понимается всесторонняя защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи ИБ сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

В данном контексте основными источниками угроз в области обеспечения безопасности информационных ресурсов ОВД следует рассматривать деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях, осуществляемого в обход установленного порядка или вопреки общепринятым нормам морали и нравственности, а также нарушение функционирования информационной инфраструктуры.

По цели воздействия выделяют три основных типа угроз безопасности ИС: нарушения конфиденциальности информации, нарушения целостности информации, нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение информации ограниченного распространения. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей ИС.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ИС, либо блокируют доступ к некоторым ее ресурсам. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Согласно Концепциии информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2018 г. №1, защищенность информации достигается комплексом мер, реализуемых функционированием системы обеспечения ИБ. В свою очередь, **система обеспечения ИБ** является совокупностью правовых, организационных и технических мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам ИБ с целью предотвращения либо существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней.

Ключевым локальным актом Министерства внутренних дел Республики Беларусь, охватывающим весь комплекс вышеуказанных мер по обеспечению ведомственной ИБ, является приказ Министерства внутренних дел Республики Беларусь от 30 сентября 2022 г. № 256 «О единой цифровой платформе Министерства внутренних дел». Данным приказом утверждена политика ИБ единой цифровой платформы Министерства внутренних дел (далее – ЕЦП МВД), устанавливающая совокупность правил, требований и руководящих принципов в области ИБ, обязательных для исполнения сотрудниками.

Основными целями указанной Политики являются:

защита активов ЕЦП МВД от случайного или преднамеренного воздействия на информацию, носители информации, процессы обработки и передачи с целью исключения возможного нанесения ущерба или уменьшения результатов его воздействия;

обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

снижение уровня рисков, связанных с ИБ;

формирование и регламентирование единых подходов и требований по обеспечению ИБ сотрудниками, а также государственными органами и организациями, иными юридическими лицами в рамках информационного взаимодействия с МВД и др.

Задачами указанной Политики являются:

определение ответственности и обязанностей участников информационных отношений по обеспечению и соблюдению требований данной Политики, в том числе с использованием программных, программно-аппаратных средств технической защиты информации;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ;

своевременное выявление и оценка источников и характера угроз ИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем МВД, и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

защита от вмешательства в процесс функционирования ЕЦП МВД посторонних лиц;

разграничение и обеспечение доступа пользователей к ИС в соответствии с их должностными обязанностями;

защита от несанкционированной модификации информации, хранящейся и обрабатываемой в ИС ЕЦП МВД, от внедрения несанкционированных программ, в том числе вредоносных, и устройств в ЕЦП МВД;

ЗИ от утечки при ее обработке, хранении и передаче по техническим каналам связи и др.

Выделим организационные и технические меры обеспечения ИБ ЕЦП МВД:

идентификация и аутентификация пользователей различных субъектов информационных отношений при обеспечении ИБ ЕЦП МВД;

управление доступом к активам;

сбор и мониторинг (просмотр, анализ) событий ИБ;

реагирование на инциденты ИБ и управление ими;

защита от вредоносного программного обеспечения;

управление информационными потоками и обеспечение сетевой безопасности;

управление процедурами резервного копирования;

обнаружение утечек защищаемой информации;

регламентация и контроль использования носителей информации, мобильных технических средств, ведомственной электронной почты;

взаимодействие с государственными органами и организациями по вопросам обеспечения ИБ;

осуществление проверочных мероприятий с целью выявления недостатков в системе ИБ МВД и др.

Объектами защиты системы ИБ ЕЦП МВД являются:

информация, хранящаяся и обрабатываемая в ИС ЕЦП МВД в соответствии с отнесенным к классам типовых ИС;

ИС, содержащие информацию, распространение и (или) предоставление которой ограничено.

В соответствии с Инструкцией о порядке организации и функционирования ведомственных сетей передачи данных, глобальной компьютерной сети Интернет, файлообменного сервиса и ведомственной электронной почты, утвержденной приказом МВД Республики Беларусь от 17.10.2024 № 349 (далее – Инструкция), пользователь ведомственной сети передачи данных (далее – ВСПД) обязан:

сообщать администратору об отказах в работе ВСПД;

не допускать использование без получения соответствующего разрешения своего СВТ другими пользователями;

сохранять в тайне личный пароль доступа к СВТ, подключенному к ВСПД, и не сообщать его другим лицам;

вводить личный пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

немедленно заменить пароль, если он был скомпрометирован;

при оставлении без присмотра включенного СВТ ограничивать его использование посторонними лицами (путем временной блокировки экрана, клавиатуры и так далее);

не использовать СВТ в сети без установленного антивирусного ПО, определяемого ЛПА в области ЗИ;

контролировать работоспособность антивирусного ПО, в том числе актуальность антивирусных баз (не более 14 дней);

немедленно ставить в известность сотрудников подразделения ИТ о ненадлежащей работе ПО, СВТ или ВСПД;

строго выполнять все требования администратора в рамках выполнения требований настоящей Инструкции.

37. Пользователь ВСПД должен немедленно поставить в известность сотрудника подразделения ИТ в случае обнаружения:

факта использования без получения соответствующего разрешения своего СВТ другими пользователями, немедленно сообщать своему непосредственному начальнику, а если указанный факт происходит с его ведома – вышестоящему руководителю;

нарушений целостности (гарантийных) пломб, нарушений или несоответствий номеров печатей на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к СВТ;

отклонений в работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ.

38. Пользователю ВСПД запрещается:

фиксировать персональные учетные данные (логины, пароли и иное) в бумажной, электронной формах или другом виде, доступном для иных лиц;

использовать ВСПД в целях, противоречащих законодательству или не связанных с выполнением должностных обязанностей;

использовать чужие учетные данные для авторизации;

просматривать, изменять и (или) копировать служебную и иную информацию других пользователей, кроме случаев, если эти действия санкционированы сотрудником, предоставившим данную информацию, либо его руководителем;

удалять установленное другими пользователями ПО;

осуществлять перенастройку любого ПО (в том числе ОС) путем изменения файлов настройки или иным образом, влияющую на работоспособность ВСПД, без согласования с подразделением ИТ;

самовольно модернизировать, заменять средства телекоммуникации, подключать к ВСПД и СВТ любые каналообразующие и коммутационные средства связи и автоматизации, в том числе мобильные телефоны, а также вносить изменения в конструкцию СВТ и других узлов ВСПД;

копировать, обрабатывать и хранить на СВТ неслужебную информацию;

подключаться к информационным ресурсам ОВД (ВВ), если это противоречит требованиям ЛПА, в том числе настоящей Инструкции;

умышленно использовать недокументированные свойства и ошибки ПО или настройки ВСПД, которые могут привести к возникновению неправильной работы или к угрозе безопасности ВСПД. При обнаружении таких ошибок пользователь обязан проинформировать начальника своего структурного подразделения и администратора.

Необходимо помнить, что соблюдение мер ИБ в повседневной деятельности сотрудника ОВД подразумевает выполнение соответствующих требований не только в служебное время, но и в нерабочее, в быту. Особое значение данная проблема приобретает в связи с активным использованием в повседневной деятельности различных информационно-коммуникационных технологий (интернет, электронная почта, социальные сети, мессенджеры, облачные хранилища и др.). С одной стороны, указанные технологии предоставляют разнообразные возможности для удобной обработки, хранения, восприятия и передачи информации. С другой стороны, они обладают широким спектром различного рода уязвимостей, существенно снижающих уровень ИБ их пользователя.

В этой связи, практические рекомендации по обеспечению ИБ сотрудника в повседневной деятельности и в быту можно представить в виде совокупности следующих мероприятий, направленных на повышение ***цифровой грамотности***.

Безопасность электронной почты (E-mail):

подключить двухфакторную аутентификацию;

использовать надежный пароль для доступа к E-mail;

использовать спам-фильтры;

использовать как минимум два типа отдельных e-mail адресов: закрытые (только для интернет-банкинга, привязки устройств и средств защиты и т. д.), открытые (только для переписки, регистрации на форумах и социальных сетях, оформления различных подписок и т. д.);

в случае подозрительных ситуаций проверить статистику подключений и изменить пароль.

Не рекомендуется реагировать на письма от неизвестных отправителей, открывать подозрительные вложения к письму (при необходимости вложенные ссылки либо файлы следует проверять на наличие вирусов с помощью специализированных онлайн-сервисов, а также отправлять в открытом виде важные данные (фотоизображения документов, пароли и т. д.).

Безопасность средств парольной защиты:

создавать персональные (уникальные) пароли к разным сервисам;

использовать сложные пароли (например, одновременно будут строчные и заглавные буквы, цифры, специальные знаки (~ ! @ # $ % & *);

регулярно производить смену паролей.

Не рекомендуется: хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо; использовать повторения символов; использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т. д.); сохранять пароль автоматически в браузере; использовать биографическую информацию и сведения, размещенные в социальной сети.

Безопасность в сети Интернет:

использовать только защищенное соединение HTTPS (проверять, чтобы в адресной строке браузера была зеленая или серая иконка замка);

производить регулярное обновление антивирусного программного обеспечения;

обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта), в результате чего могут быть скомпрометированы ваши логин, пароль и иные критически важные данные;

отключить общий доступ и использовать надежный пароль для доступа к вашей Wi-Fi точке;

деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам;

осуществлять проверку на наличие чужих (не доверенных) устройств в списке подключенных клиентов на роутере.

Не рекомендуется: переходить по непроверенным ссылкам и посещать сайты сомнительного содержания; открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами программное обеспечение; вводить свой логин и пароль доступа к учетной записи (странице) или системе дистанционного банковского обслуживания при подключении к

бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т. д.

Использование социальных сетей и мессенджеров:

целесообразно скрывать персональную и контактную информацию о себе (номер телефона, адрес электронной почты, цифровое фото и другие сведения) в открытом доступе (аккаунт в социальной сети рекомендуется сделать закрытым);

обмениваться сообщениями в социальных сетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.

Не рекомендуется: использовать указание геолокации на фото и постах; размещать в сети Интернет объявления с указанием используемых номеров телефонов, а также указывать контактные данные мессенджеров (в случае размещения – удалять сразу же по миновании надобности).

Безопасность мобильных устройств:

использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль и др.);

своевременно обновлять операционную систему устройства, антивирусное и иное программное обеспечение;

устанавливать приложения только из проверенных источников;

обращать внимание, к каким функциям гаджета приложение запрашивает доступ;

включить встроенные функции устройства для определения его местонахождения;

в случае утери (хищения) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам;

при смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно);

при продаже устройства произвести его сброс до заводских настроек.

Не рекомендуется: передавать незнакомым мобильный телефон или сим-карту (в случае передачи – контролировать все действия, которые производятся с устройством); устанавливать приложения с низким рейтингом и отрицательными отзывами; перезванивать на незнакомые иностранные номера; хранить важную информацию на мобильном устройстве; делать полное снятие ограничений на устройстве.

Получение достоверной информации

В контексте развития и повсеместного использования нейросетевых технологий, способных генерировать фото и видеоконтент о событиях, не имевших место в действительности, а также с использованием изображений лиц, не имеющих отношение к произошедшим событиям, особую актуальность приобретает умение отличать достоверную информацию от дипфейков. Дипфейк – это методика синтеза изображения, основанная на искусственном интеллекте. Методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или

видеоролики. Для того, чтобы удостовериться в оригинальности информации необходимо произвести ее верификацию.

Верификация – простыми словами, это технология проверки информации на достоверность, правильность, точность. Верификация не обязательно сложна. Для нее не требуется сложных алгоритмов или доступа к продвинутым инструментам или программам, которые автоматически определяли бы, является ли снимок фейком или манипуляцией.

Наиболее распространенными видами недостоверной информации, которую можно выявить проведя верификацию, являются:

1. Неверное время/неверное место

Самый распространенный вид недостоверной информации – это вырванные из контекста фотографии или видео, которые повторно публикуются в сети с связи с актуальными событиями. Такие сведения часто распространяют в социальных сетях без злого умысла. Обнаружить фальсификацию, как правило, легко, если следовать некоторым правилам.

2. Фотошоп и монтаж

Более редки случаи с подделкой изображений в фотошопе или видеомонтажом. Такие материалы часто публикуются намеренно, для того, чтобы ввести людей в заблуждение. Обнаружить подделку такого типа может быть сложнее, чем установить недостоверную ошибку вида «неверное время/ неверное место».

3. Подделка

Подделка встречается реже всего, поскольку для ее производства требуются большие усилия. Такие материалы специально публикуют для того, чтобы ввести людей в заблуждение. Встречаются разные типы подделок.

4. Постановочное видео

Постановочное видео может выглядеть как настоящая запись, при этом зачастую генерируется нейросетью либо производится профессиональным режиссером, а в съемке участвуют актеры.

5. Сайты с поддельными новостями

Сайты с поддельными новостями имитируют реальные новостные издания. Их успешно используют для того, чтобы запустить виральные истории в сеть. Эти сайты могут повторять внешний вид реальных изданий; отличить их можно с помощью информации в URL.

6. «Местечковые вирусные истории»

«Местечковые вирусные истории» – это своего рода новый тренд. Сайты с вымышленными новостями публикуют новости о событиях, произошедших в конкретных населенных пунктах: от террористических атак до ссор знаменитостей. Источники этих историй всегда крайне сомнительны, но иногда местные СМИ подхватывают эти истории и публикуют как настоящие.

Существует простая инструкция по верификации фотографий и видео, которая поможет в спорных ситуациях. Инструкция из пяти шагов поможет проверить как источник, так и содержание, просто ответьте на вопросы:

1. Имеете ли вы дело с оригиналом?

2. Знаете ли вы, кто сделал фото/видео?
3. Знаете ли вы, где было сделано фото/видео?
4. Знаете ли вы, когда было сделано фото/видео?
5. Знаете ли вы, почему было сделано фото/видео?

Учитывая, что наиболее распространенные виды подлога – это старые видео и фото, которые распространяют в привязке к актуальным событиям и новостям, то при проверке важно убедиться в том, что материал является или оригинальным (то есть он не публиковался в интернете раньше и не подвергался обработке) или настолько близким к оригиналу, насколько можно найти.

Найти оригинал можно, воспользовавшись следующими способами:

обратный поиск изображений через Google Image Search или TinEye и др;

проверка видео через сервисы Data Viewer;

проверка теней и отражений;

при общении с источником попросите его прислать исходный файл (с EXIF данными) и проанализируйте в них дату и место сьемки;

используйте инструменты анализа изображений – например, Izitru или Forensically, чтобы выявить признаки обработки (лучше всего проверять исходники изображений, а не файлы, найденные в социальных сетях).

Резюмируя, уместно кратко изложить базовые правила безопасности в контексте цифровой грамотности сотрудников ОВД:

1. Не отвечать на не ожидаемые телефонные звонки с абонентских номеров иностранных государств, в том числе поступающие в мессенджерах.
2. Не переходить по «подозрительным» ссылкам.
3. Использовать различные пароли для различных ресурсов, стараясь самостоятельно либо с использованием программного обеспечения генерировать «сложные» пароли, содержащие символы верхнего и нижнего регистра, цифры, специальные символы.
4. Не использовать при создании пароля своей фамилии, имени, даты рождения и иных общеизвестных символов.
5. Не хранить пароли в общедоступных ресурсах.
6. Не сообщать пароли и персональные данные третьим лицам.
7. Не пользоваться ресурсами теневого сегмента сети Интернет – так называемый Даркнет.
8. Всегда проверять информацию на официальных ресурсах государственных органов, банков и небанковских кредитно-финансовых организаций.
9. Контролировать посещение детьми ресурсов в сети Интернет, в том числе с использованием функции «Родительский контроль».
10. Обучать родственников пожилого возраста особенностям работы в сети Интернет, объяснять им правила безопасности.

Использование двухфакторной аутентификации или 2FA (метод проверки личности пользователя, при котором два из трех возможных факторов аутентификации объединяются для предоставления доступа к веб-сайту или

приложению).

Список использованных источников

1. О единой цифровой платформе Министерства внутренних дел : приказ МВД Республики Беларусь от 30 сентября 2022 г., № 256;

2. Симхович, В. А. Цифровая грамотность населения Беларуси: социально-демографические характеристики / В. А. Симхович // Рос. науч. журн. «Телескоп: журнал социологических и маркетинговых исследований». – 2023. – № 4 (12). – С. 11–14.

Вопросы для самоконтроля

Что такое информационная безопасность?

Каким нормативным правовым актом регламентировано создание и использование единой цифровой платформы Министерства внутренних дел?

Что запрещается пользователю ВСПД?

Какие существуют типы угроз ИС?