Следственный комитет
Республики Беларусь
Управление по Витебской области
**БЕШЕНКОВИЧСКИЙ
РАЙОННЫЙ ОТДЕЛ**
ул. Школьная, 6, 211361, г.п. Бешенковичи
тел., факс 8 (02131) 6-34-91
e-mail: besh_vt@sledcom.by

Председателю
Бешенковичского районного
исполнительного комитета
Унукович Г.В.

Председателям Бешенковичского,
Уллльского, Островенского,
Бочейковского, Соржицкого,
Верхнекривинского, Верховского
сельских исполнительных комитетов

Учреждения (предприятия) образования,
здравоохранения, агропромышленного
комплекса, промышленности, сферы
услуг, торговли, расположенные
на территории Бешенковичского района

ИНФОРМАЦИОННОЕ ПИСЬМО
«О вопросах профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий»

В январе – сентябре 2026 года на территории Республики Беларусь отмечается сокращение количества зарегистрированных преступлений, с 46 554 до 41 785 (-10,2% по отношению к аналогичному периоду 2025 года). На территории Витебской области число зарегистрированных преступлений сократилось на 12,1% (с 5 403 до 4 747).

Показатель числа зарегистрированных преступлений, из расчета на 10 тысяч населения в Бешенковичском районе выше среднеобластного и составляет (45,4).

В сравнении с аналогичным периодом прошлого года негативными количественные показатели остаются в Витебской области по преступлениям, совершенным с использованием информационно-коммуникационных технологий (киберпреступления) – 1366 преступлений.

Киберпреступность затрагивает обычных пользователей, семьи, предприятия и государственные организации. Злоумышленники могут пытаться украсть пароли и деньги, получить доступ к личной переписке, заразить устройство вредоносной программой или использовать чужие данные для обмана. При этом многие атаки начинаются не со сложного взлома, а с сообщения, подозрительной ссылки или невнимательно настроенной учетной записи.

Как распознать распространенные киберугрозы

Фишинг – это попытка получить конфиденциальные сведения с помощью обманного сообщения или сайта. Письмо или сообщение может выглядеть как уведомление от банка, службы доставки, нанимателя, магазина или государственного учреждения. Адрес отправителя и оформление иногда похожи на настоящие, поэтому одного внешнего вида недостаточно, чтобы подтвердить подлинность сообщения.

Другой распространенный риск – вредоносное программное обеспечение. Оно может попасть на устройство через сомнительное приложение, вложение в письме, поддельное обновление или нелегальную копию программы.

Злоумышленник может представиться сотрудником банка, технической поддержки или знакомым и побуждать к срочным действиям. Давление, обещание выгоды, угроза блокировки и просьба сохранить разговор в тайне – поводы остановиться и проверить информацию через независимый канал связи.

Защита учетных записей и паролей

Для каждой важной учетной записи следует использовать отдельный пароль. Если один и тот же пароль повторяется на разных сайтах, утечка с одного сервиса может поставить под угрозу другие аккаунты. Надежный пароль должен быть достаточно длинным и непредсказуемым. Не стоит составлять его из имени, даты рождения, номера телефона или простых последовательностей символов.

По возможности включите многофакторную аутентификацию – дополнительную проверку при входе, помимо пароля. Она может использовать приложение-аутентификатор, аппаратный ключ или другой способ, предложенный сервисом. Одноразовые коды и подтверждения входа нельзя передавать другим людям, даже если собеседник представляется специалистом.

Как не стать жертвой онлайн-мошенничества

Не переходите по ссылкам из неожиданного сообщения, если оно требует срочно войти в аккаунт или оплатить услугу. Откройте приложение самостоятельно или введите адрес нужного сервиса вручную. Проверяйте доменное имя сайта: мошенники могут использовать адреса, которые отличаются от настоящих одной буквой или дополнительным словом.

Если сообщение связано с деньгами, доставкой или блокировкой аккаунта, свяжитесь с организацией по номеру телефона или через приложение, найденные независимо от сообщения. Не пользуйтесь контактами из подозрительного письма. Не сообщайте коды из SMS, данные банковской карты, пароль и коды восстановления. Не устанавливайте программы удаленного доступа по просьбе незнакомого собеседника: с их помощью он может видеть экран или управлять устройством.

При покупках в интернете проверяйте продавца, условия возврата и способы оплаты. Настороженно относитесь к предложениям с необычно низкой ценой, требованию перевести деньги на личную карту или просьбе продолжить сделку за пределами торговой площадки. Сохраняйте подтверждения оплаты и переписку. Для онлайн-платежей полезно использовать отдельную карту или счет с ограниченным балансом.

Безопасность детей, семьи и сотрудников

Детям важно объяснять правила цифровой безопасности спокойно и без запугивания. Они должны знать, что нельзя отправлять незнакомцам пароли, коды и фотографии документов, а подозрительные сообщения нужно показывать взрослому. Настройки приватности и родительского контроля помогают, но не заменяют регулярного разговора.

В семье заранее обсудите, как проверять просьбы о срочном переводе денег или передаче личных сведений. Например, можно перезвонить близкому

человеку по сохраненному номеру, а не отвечать на сообщение с неизвестного аккаунта.

В организациях профилактика включает обучение сотрудников, ограничение доступа к данным по рабочим обязанностям и понятный порядок сообщения об инцидентах. Рабочие устройства следует использовать по правилам организации, а подозрительные письма – передавать ответственному специалисту, не открывая вложения. Важно, чтобы сотрудник мог быстро сообщить об ошибочном переходе по ссылке или раскрытии пароля: раннее сообщение помогает быстрее ограничить последствия.

Что делать при подозрении совершения киберпреступления

Если вы ввели пароль на подозрительном сайте, смените его через официальный сайт или приложение. Если этот пароль использовался в других сервисах, замените его и там. Завершите активные сеансы, проверьте способы восстановления доступа и включите многофакторную аутентификацию. Если затронуты банковские данные, немедленно свяжитесь с банком по официальному номеру и следуйте его инструкциям.

Не пытайтесь самостоятельно связываться с мошенниками и не устанавливайте программы, предложенные неизвестными лицами. Сохраните сообщения, адреса сайтов, время событий и другие подтверждения. Не удаляйте важные материалы, если они могут понадобиться для обращения в банк, службу поддержки или правоохранительные органы.

Если вы потеряли доступ к аккаунту, используйте официальную процедуру восстановления. Предупредите контакты, если от вашего имени рассылаются сообщения или просьбы о деньгах. При финансовом ущербе сообщите об этом банку и обратитесь в компетентные органы.

Профилактика киберпреступности начинается с простых и регулярных действий: уникальных паролей, дополнительной проверки входа, своевременных обновлений, осторожности при работе со ссылками и резервных копий. Не доверяйте срочным просьбам передать деньги, пароль или код, даже если сообщение выглядит убедительно. Проверяйте информацию через независимые официальные каналы и быстро сообщайте о подозрительных действиях. Последовательное соблюдение этих правил снижает риск кражи данных и денег и помогает быстрее восстановить безопасность, если инцидент все же произошел.

Просим довести указанную информацию до всех сотрудников (работников) Вашей организации (учреждения, предприятия).

С уважением,

Начальник
Бешенковичского районного отдела
Следственного комитета
подполковник юстиции П.Ю. Войткус
30.09.2026