Radio Frequency Service

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РАБОТНИКОВ РГП “ГРС” ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ

## КИБЕРБЕЗОПАСНОСТЬ ГОСУДАРСТВА – ЭТО ОТВЕТСТВЕННОСТЬ КАЖДОГО ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО

Кибербезопасность – состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз

## ПОЧЕМУ ВАЖНО ОБЕСПЕЧИВАТЬ КИБЕРБЕЗОПАСНОСТЬ?

1. Киберпространство становится все более важным как для функционирования государств, так и для предоставления государственных услуг гражданам.
2. Кибератаки наносят экономический ущерб, подрывают общественное доверие к онлайн-услугам и наносят реальный вред гражданам, их собственности и конфиденциальности.
3. Кибератаки становятся возможными преимущественно из-за человеческой халатности и неосторожности: слабые пароли, разглашение личных данных.


## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: **конфиденциальность, целостность и доступность.**

**Конфиденциальность** информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

**Целостность** информации – способность информации (данных) сохраняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к нарушению целостности.

**Доступность** информации определяется способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводят к потере доступности.


## КЛЮЧЕВЫЕ ПРОБЛЕМЫ

- низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности;
- нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;
- непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;
- действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;
- деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

## ТИПЫ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

1. **Программа-вымогатель** – разновидность вредоносного программного обеспечения для вымогательства денег посредством блокировки доступа к файлам компьютерной системы до поступления выкупа. Перечисление выкупа не гарантирует восстановление файлов или работоспособности системы.

2. **DDoS- атака** (с англ. Distributed Denial of Service – «отказ от обслуживания») – распределенная атака типа отказ в обслуживании, которая являет собой одну из самых распространенных и опасных сетевых атак. В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов. В результате DDoS-атаки сервера, обслуживающие сайты вынуждены обрабатывать чрезмерный объём ложных запросов и сайт становится недоступным для простого пользователя.

3. **Социальная инженерия** – тактика, которую используют злоумышленники, чтобы склонить пользователя к раскрытию конфиденциальной информации.

4. **Фишинг** (англ.phishing, от fishing – рыбная ловля, выуживание) – вид компьютерного мошенничества, основная цель которого – обманным путем вынудить жертву предоставить мошеннику нужную информацию. Это компьютерное преступление, которое преследуется по закону.

5. **Взлом сайта** – это получение злоумышленником несанкционированного доступа к файлам сайта или к разделу администрирования системы управления сайтом.


# ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

**Вредоносное программное обеспечение** (maleware – сокращение от malicious software: **malicious** – злонамеренный и **software** – программное обеспечение) – общепринятый термин, используемый для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу или компьютерной сети.

Вредоносные программы представляют собой широкую категорию программного обеспечения. Они устанавливаются без Вашего разрешения и влияют на работу Вашего компьютера.

По методу распространения выделяют следующее вредоносное ПО: эксплоиты, логические бомбы, троянские и шпионские программы, компьютерные вирусы и сетевые черви.

**Троян**- вредоносная программа используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

**Компьютерный вирус** – разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации). В дополнение к этому он может повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого запущена заряжённая программа.

**Сетевой червь** – разновидность самовоспроизводящейся компьютерной программы, распространяющейся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов червь является самостоятельной программой. Trackware – новая вариация вредоносной программы которая отслеживает и регистрируют действия, производимые на компьютере.

## КАКИМ ОБРАЗОМ ВРЕДОНОСНЫЕ ПРОГРАММЫ ПРОНИКАЮТ НА КОМПЬЮТЕР ПОЛЬЗОВАТЕЛЯ?

Вредоносные программы, чаще всего, проникают на компьютер через Интернет или по электронной почте. Если Вы сделаете ошибку в URL- адресе или случайно нажмете на известную ссылку, то можете попасть на опасные сайты с «агрессивным» содержания или вредоносными программами. P2P (peer-to-peer) сети, в которых пользователи могут передавать файлы непосредственно с одного компьютера на другой, представляют существенный риск для заражения компьютера вредоносным и рекламным ПО.

## КАК ВРЕДОНОСНЫЕ ПРОГРАММЫ ВЛИЯЮТ НА РАБОТУ КОМПЬЮТЕРА?

Симптомами заражения вредоносной программой являются всплывающие окна, снижение работоспособности системы или перенаправление запросов в браузере на нежелательные сайты. Вредоносные программы влияют на нормальное функционирование системы, что может привести к отказу в обслуживании, замене данных и понижению пропускной способности сети. Кроме того, компьютер будет невозможно выключить или перезагрузить.

## КАК ЗАЩИТИТЬ КОМПЬЮТЕР ОТ ВРЕДОНОСНЫХ ПРОГРАММ?

Вредоносные программы зачастую распространяются в приложении с другими файлами, так что не открывайте вложения электронной почты, отправленные с неизвестных Вам ресурсов. Никогда не принимайте файлы от незнакомых Вам пользователей, а также проявляйте осторожность, когда открываете файлы с расширением AVI,EXE или JPG.

## ЕСЛИ ВЫ ПОДОЗРЕВАЕТЕ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН ВРЕДОНОСНОЙ ПРОГРАММОЙ:

Приостановите любую деятельность, которая связана с использованием логинов, паролей и другой конфиденциальной информации.

Используйте антивирусное ПО для защиты Вашей системы от возможных онлайн-угроз. Установите антивирусные и антишпионские программы из надежных источников.

Убедитесь, что Ваша антивирусная программа обновлена, сканирует компьютер и удаляет все программы, которые определяются как вредоносные. Зачастую, в спешке можно невнимательно прочитать всплывающее сообщение, которое содержит неверную информацию об окончании проверки компьютера и обнаружении проверки компьютера и обнаружении вредоносных программ. В подобном сообщении предлагается загрузить фальшивое программное обеспечение, которое широко используется для распространения вредоносных программ.

## РЕГУЛЯРНО ОБНОВЛЯЙТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Киберпреступники крайне изобретательны в своих попытках использовать уязвимости в программном обеспечении. Поэтому необходимо:

- Регулярно устанавливать обновления для всего вашего программного обеспечения - антивирусных и антишпионских программ, операционных систем, программ обработки текстов и прочих программ.
- Включать функции автоматического обновления программного обеспечения, когда таковое доступно.
- Удалить программное обеспечение, которое вы не используете.

## ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ И ХРАНИТЕ ИХ В СЕКРЕТЕ

- Надежные пароли должны состоять минимум из 8 символов и содержать сочетание букв, цифр и символов.
- Никому не раскрывайте свои пароли.
- Не используйте одинаковый пароль на всех сайтах. Если его украдут, вся информация подвергнется риску.
- Создавайте разные надежные пароли для маршрутизатора и ключ беспроводного соединения дома. О том, как это сделать, узнайте в компании, представляющей маршрутизатор.

## НИКОГДА НЕ ОТКЛЮЧАЙТЕ БРАНДМАУЭР

Брандмауэр создает защитный заслон между вашим компьютером и Интернетом. Выключение брандмауэра даже на минуту увеличивает риск заражения ПК вредоносной программой.

## ОСТОРОЖНО ИСПОЛЬЗУЙТЕ ФЛЕШ-НАКОПИТЕЛИ

Минимизируйте возможность заражения компьютера вредоносным ПО:

- Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер.
- Зажимайте клавишу SHIFT, когда вы вставляете накопитель в компьютер. Если вы забыли это сделать, нажмите в верхнем правом углу, чтобы закрыть всплывающие окна флеш-накопителя.
- Не открывайте неизвестные файлы на накопителе.

## НЕ СОГЛАШАЙТЕСЬ НА ЗАГРУЗКУ, ПРЕДЛАГАЕМУЮ ВРЕДОНОСНЫМ ПО

- Будьте очень внимательны, открывая вложенные файлы или нажимая на ссылки в электронной почте, мгновенных сообщениях или в публикациях в социальных сетях – даже если вы знаете отправителя. Если отправил друг, позвоните ему и узнайте, он ли это сделал: если нет, удалите или закройте окно службы обмена мгновенными сообщениями.
- Не нажимайте кнопки **«Согласен»**, **«ОК»** и **«Я принимаю»** в баннерной рекламе, в неожиданных всплывающих окнах или предупреждениях, на сайтах, которые кажутся незаконными, или в предложениях удалить шпионские ПО или вирусы.
- Нажмите **CTRL+F4** на клавиатуре.
- Если окно не закрывается, нажмите **Alt+F4** на клавиатуре, чтобы закрыть браузер. Если необходимо, закройте все вкладки и не сохраняйте вкладки для следующего запуска браузера.
- Загружайте программное обеспечение только на сайтах, которым вы доверяете.
- Не переходите по ссылкам в сообщениях электронной почты и избегайте веб-сайтов, где предлагается бесплатное программное обеспечение — особенно бесплатное антивирусное ПО. Остерегайтесь «бесплатных» загрузок музыки, игр, видео и всего прочего. Они могут содержать вредоносное ПО в загрузке.

# РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

## Парольная политика

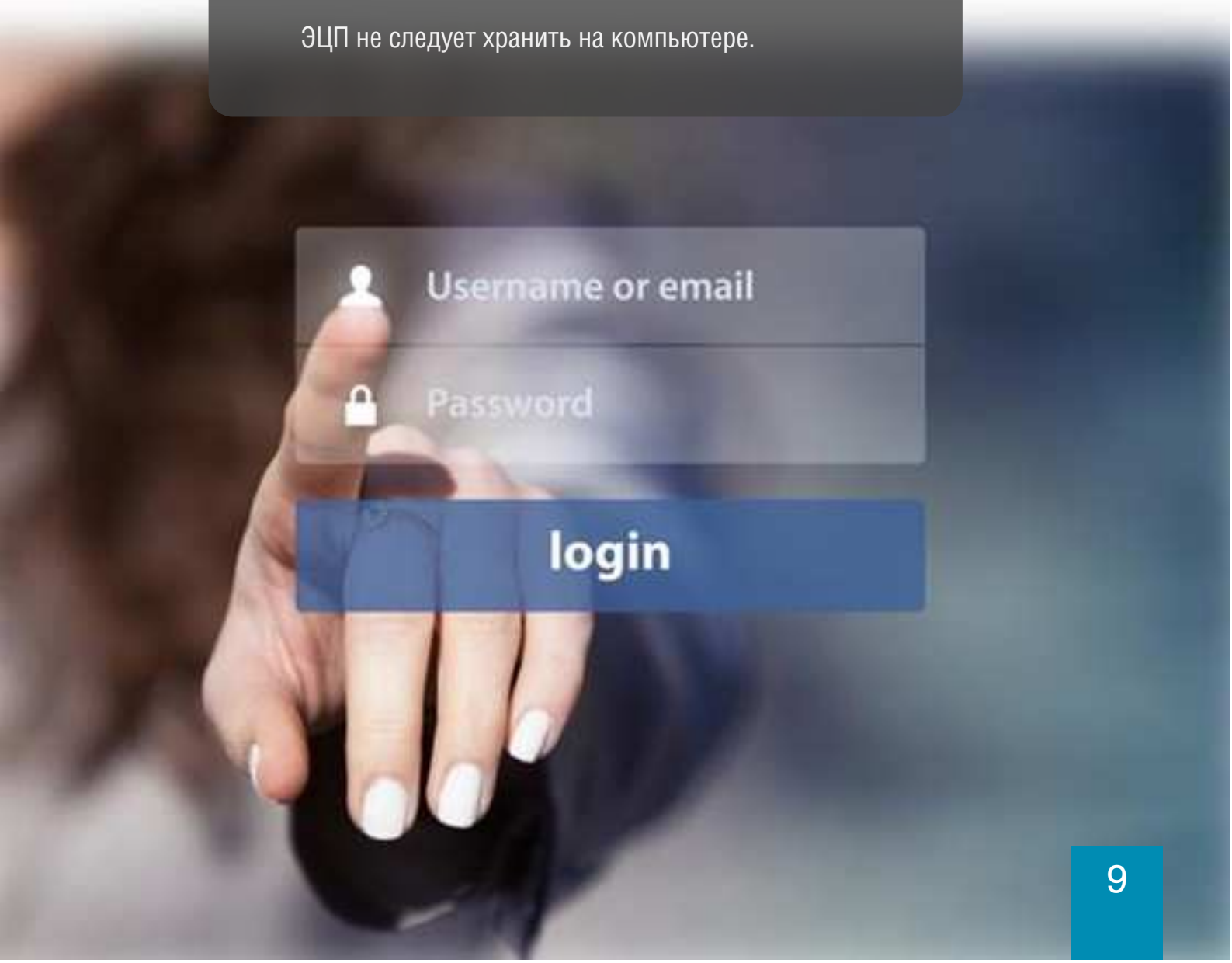
1. Не сохранять пароли в электронном виде на рабочем столе, не хранить записанные пароли в общедоступных местах, не сообщать пароли третьим лицам.

2. Допускается раскрытие значений пароля в случае производственной необходимости, после чего необходимо ОБЯЗАТЕЛЬНО сменить пароль.

3. Пароли должны быть не меньше 8 символов и должны обновляться ежеквартально.

## Электронная цифровая подпись

ЭЦП не следует хранить на компьютере.



# РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

## Почта

1. Не открывать от незнакомых лиц электронные письма и подозрительные вложения, особенно если это архивы или исполняемые файлы (.exe). Если Вы считаете, что письмо важное, то необходимо связаться с отправителем по телефону и уточнить тему письма и причину отправки.

2. На любой подозрительный запрос по электронной почте необходимо использовать альтернативный канал связи (к примеру, телефон), чтобы подтвердить запрос у адресата.

3. Необходимо всегда проверять правильность написания адреса отправителя и получателя (даже тех, с кем вы переписываетесь ежедневно).

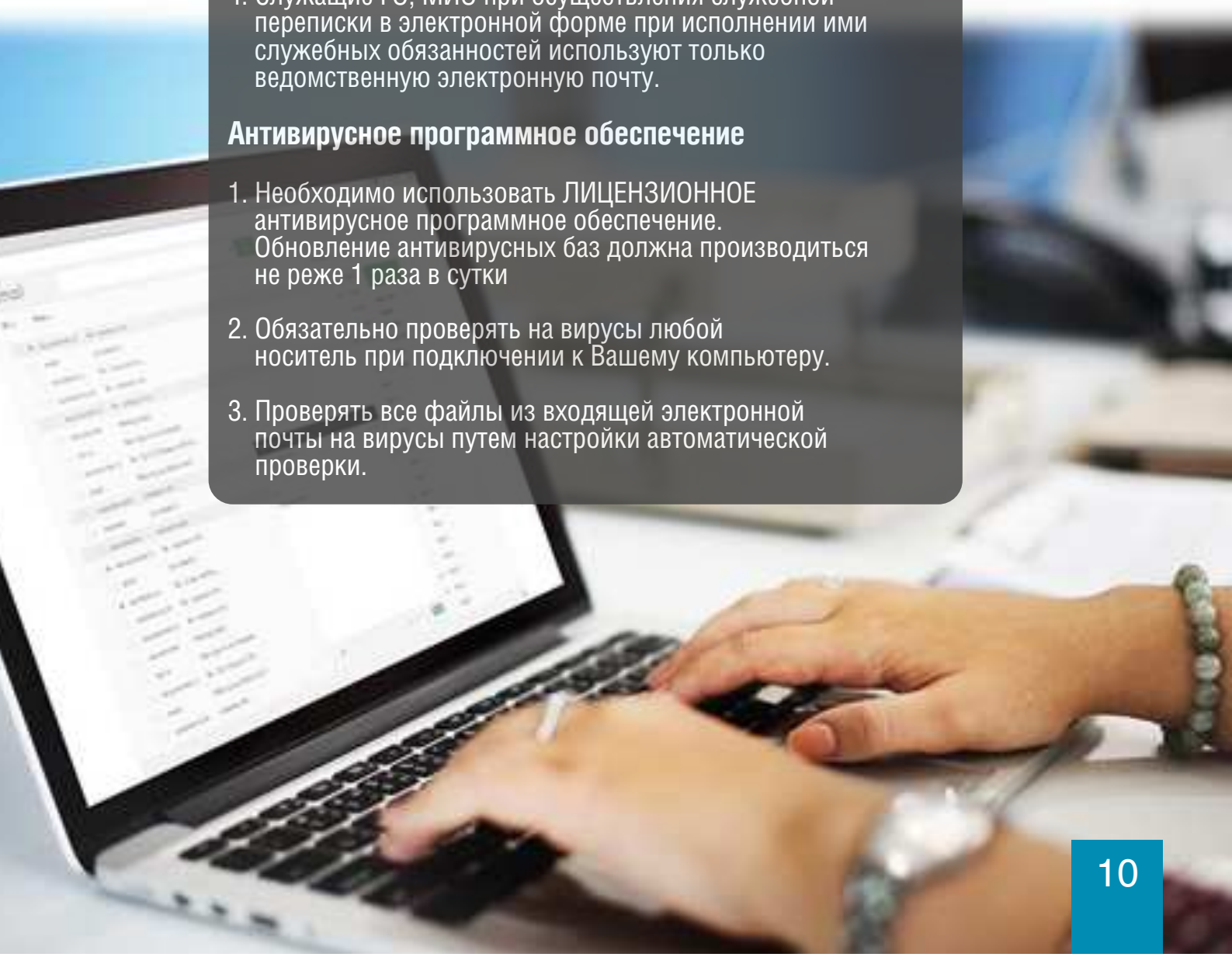
4. Служащие ГО, МИО при осуществления служебной переписки в электронной форме при исполнении ими служебных обязанностей используют только ведомственную электронную почту.

## Антивирусное программное обеспечение

1. Необходимо использовать ЛИЦЕНЗИОННОЕ антивирусное программное обеспечение. Обновление антивирусных баз должна производиться не реже 1 раза в сутки

2. Обязательно проверять на вирусы любой носитель при подключении к Вашему компьютеру.

3. Проверять все файлы из входящей электронной почты на вирусы путем настройки автоматической проверки.



# РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

## Интернет и социальные сети

1. Подключение к сети Интернет необходимо проводить только через Единый шлюз доступа к Интернету.
2. Запрещается подключать компьютер в ЕТС ГО[1] к сети Интернет. Необходимо использовать отдельные компьютеры для каждой сети.
3. Запрещается подключение к ЕТС ГО, локальной сети ГО посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи, абонентских устройств сотовой связи и других беспроводных сетевых устройств.
4. Не допускается переходить по ссылкам и запускать программы, полученные по электронной почте от неизвестного отправителя.
5. Запрещается посещать веб-сайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности.
6. Запрещается посещать сомнительные и вредоносные сайты, а также сайты, информация на которых не связана с исполнением функциональных обязанностей.
7. Запрещается принимать соглашения при посещении сайтов, смысла которых Вы не понимаете.
8. Запрещается использовать пароли доступа в локальную сеть в других программах и на сайтах, где требуется регистрация.
9. При работе с ресурсами сети Интернет и электронной почтой запрещается разглашение государственной, служебной и коммерческой информации, ставшей известной сотруднику по служебной необходимости либо иным путем.
10. Во избежание угроз, связанных с использованием cookies рекомендуется периодически проводить анализ сохраненных cookies, с целью выявления наличия в них ценной конфиденциальной информации.

---

[1] **Единая транспортная среда государственных органов (ЕТС ГО) - сеть телекоммуникаций, входящая в информационно-коммуникационную инфраструктуру «электронного правительства» и предназначенная для обеспечения взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету),**

# РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

## Социальная инженерия

1. Запрещается оставлять включенными без присмотра компьютеры, подключенные к ЕТС ГО и Интернет-сети в открытом виде. В случае оставления рабочего места в обязательном порядке необходимо блокировать компьютер (быстрый способ блокирования компьютера – комбинация клавиш Windows+L).

2. Запрещается сообщать третьим лицам IP-адреса и сочетание логина и пароля.

3. Запрещается устанавливать самостоятельно программное обеспечение и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение.

**При любых нестандартных ситуациях или при подозрении на нарушение кибербезопасности необходимо обратиться к ответственным специалистам по информационной безопасности ГО и в Службу реагирования на компьютерные инциденты по телефону +7 (7172) 55-99-97, info@kz-cert.kz.**

## НОРМАТИВНЫЕ И ПРАВОВЫЕ АКТЫ

**Закон Республики Казахстан** от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» регулирует общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а также при государственной поддержке развития отрасли информационно-коммуникационных технологий. Внесены изменения и дополнения согласно Закону Республики Казахстан от 28 декабря 2017 года № 128-VI ЗРК.

**Постановление Правительства** Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» регулирует Единые требования(ЕТ) в области информационно-коммуникационных технологий и обеспечения информационной безопасности.
ЕТ определяют требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

**Концепция кибербезопасности (Киберщит Казахстана)** разработана в соответствии с Посланием Президента Республики Казахстан Третья модернизация Казахстана: Глобальная конкурентоспособность с учетом подходов Стратегии Казахстан-2050 по вхождению Казахстана в число 30-ти самых развитых государств мира. Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.