Методические рекомендации по работе в единой информационно-телекоммуникационной сети Правительства края

1. Общие положения

1.1. Настоящие рекомендации разработаны в целях совершенствования защиты информации и повышения осведомленности в области защиты информации сотрудников (далее – пользователи) исполнительных органов края (далее – ИОК), администрации Губернатора и Правительства края (далее – администрация), использующих в своей работе средства вычислительной техники (далее – СВТ).

17.07.2024 23031-1-52

1.2. В рекомендациях рассматриваются методы и приемы безопасной работы на СВТ при выполнении служебных обязанностей.

1.3. При возникновении проблем, описанных в настоящих рекомендациях и им подобных, следует обращаться только к уполномоченным лицам. Самостоятельное решение возникших проблем может повлечь за собой возможное ухудшение работоспособности и защищенности СВТ.

2. Общие принципы работы пользователя СВТ

2.1. Пользователю следует:

– обеспечивать сохранность выданных ему СВТ, служебных машинных носителей информации (далее – МНИ), персональных идентификаторов (token, смарт-карты, iButton и т.п.);

– обеспечивать конфиденциальность информации, хранимой на выданных МНИ;

– использовать выданные ему СВТ и МНИ исключительно в целях выполнения своих должностных обязанностей (вся информация, находящаяся на МНИ должна быть служебного характера, запрещено использовать служебные МНИ для передачи файлов в личных целях);

– при использовании ключей электронной подписи в нерабочее время обеспечить хранение ключей в надежно запираемых (желательно опечатываемых) ящиках, шкафах, сейфах;

– при оставлении рабочего места блокировать компьютер путем штатной блокировки рабочего места (комбинация клавиш Win+L);

– контролировать действия лиц в рабочих кабинетах, не имеющих право самостоятельного доступа в эти кабинеты (посторонние посетители);

– размещать экран монитора таким образом, чтобы исключить несанкционированный просмотр информации с него посторонними лицами;

– своевременно сообщать ответственному за обеспечение безопасности информации в ИОК или администрации о выявленных фактах нарушений, установленных настоящей инструкцией требований по обеспечению безопасности информации.

2.2. Пользователю не допускается:

– подключать к компьютеру личные съемные устройства хранения информации (МНИ, сотовые телефоны, смартфоны, планшеты, карты памяти

через кард-ридеры, USB-модемы (3G, 4G/LTE), USB Wi-Fi/Bluetooth адаптеры и т.п.);

– выбрасывать вышедшие из строя служебные съемные МНИ. При выходе из строя служебных съемных МНИ необходимо их передать сотруднику, ведущему учет съемных МНИ, с отметкой (собственноручная подпись) в соответствующем журнале;

– разглашать информацию, доступ к которой ограничен федеральным законами;

– передавать свои учетные данные (имена учетных записей и пароли к ним) третьим лицам;

– совершать любые попытки повышения пользовательских привилегий;

– выбрасывать бумажные носители со служебной информацией (например, парольные карточки с разовыми паролями, телефонный справочник ИОК и администрации с их контактными данными и т.п.), в том числе и документы с пометкой "для служебного пользования". Такие документы подлежат уничтожению в специализированных бумагорезательных машинах;

– подключать в розетки локальной сети любые посторонние (в том числе личные) сетевые устройства.

3. Работа в сети Интернет

3.1. Основные правила работы в сети Интернет:

– не обсуждать служебные вопросы в социальных сетях, форумах и иных веб-ресурсах[1];

– не открывать веб-страницу, при попытке открытия которой выходит сообщение о том, что страница заражена вирусной программой (пример предупреждающего сообщения представлен на рисунке 1)[2];

– при использовании сайтов, поддерживающих протокол защиты трафика (далее – SSL), следует отслеживать наличие у сайта включенной защиты[3].

3.2. Метод распознавания – подлинные веб-узлы используют SSL или другие технологии безопасности для защиты личных сведений, вводимых пользователем при создании учетной записи и последующем входе на веб-узел. Если на странице используются технологии безопасности, в строке состояния обозревателя отображается значок в виде замка. Кроме того, веб-адрес содержит префикс **https://** (обращаем внимание на букву "**S**" после http, которая обозначает "безопасный") вместо обычного префикса **http://**

[1] Злоумышленник может попытаться войти в доверие для получения служебной информации или дискредитировать в сети Интернет как сотрудника ИОК или администрации, так и деятельность ИОК или администрации на основе получаемой от его сотрудника информации.

[2] Антивирусное программное обеспечение, установленное на СВТ или встроенные системы веб-фильтрации браузеров, предупреждает о том, что веб-страница заражена вирусной программой и Ваш компьютер скорее всего будет заражен при переходе на такую веб-страницу.

[3] Особенно актуально для распознавания поддельного веб-узла при использовании общедоступных ресурсов, требующих авторизацию (ввод имени учетной записи и пароля).

(рисунок 2). Префикс **https://** означает, что на веб-ресурсе используется защищенный SSL-сертификат, подтверждающий подлинность данного ресурса.

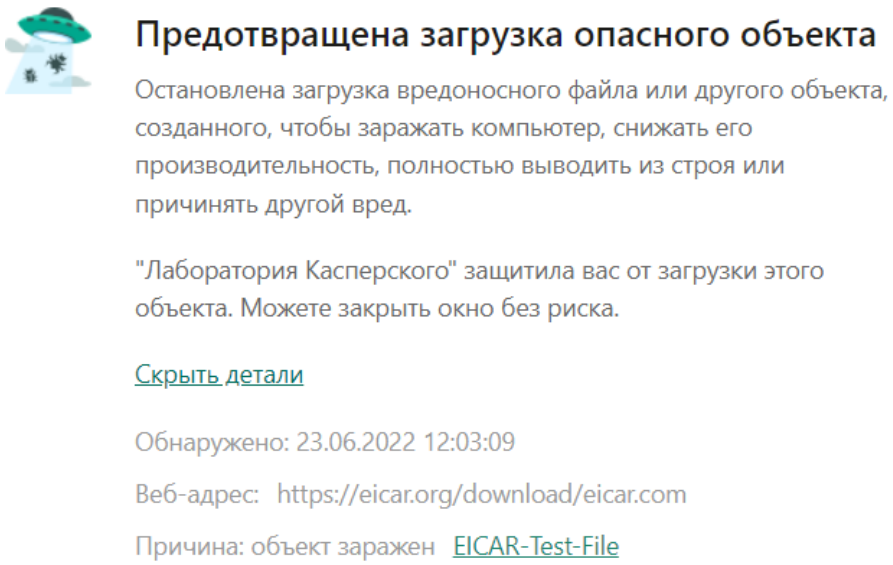

Рисунок 1 – пример предупреждающего окна

В случае неработоспособности SSL (недействительный сертификат, подмена сертификата) префикс **https://** запрашиваемого по обычной ссылке веб-ресурса может быть перечеркнут (рисунок 3) и окно браузера выводит сообщение о том, что Ваше подключение не защищено (рисунок 4).

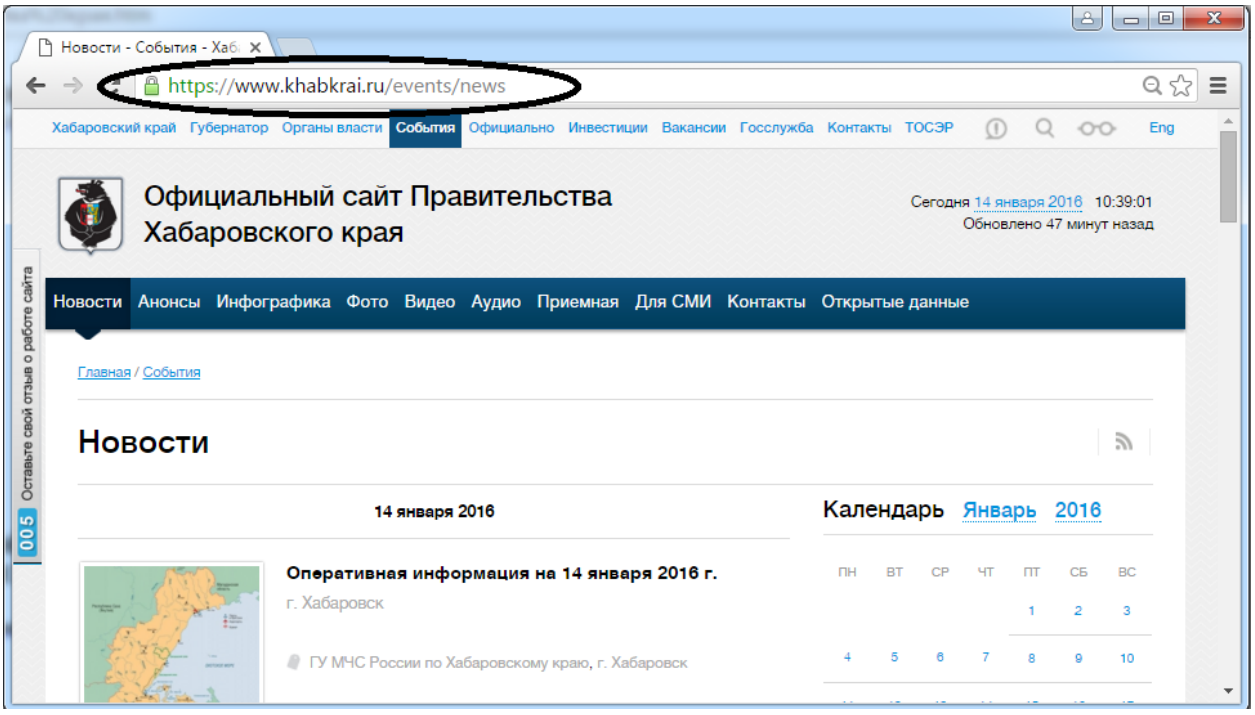

Рисунок 2 – вид адресной строки браузера при использовании SSL

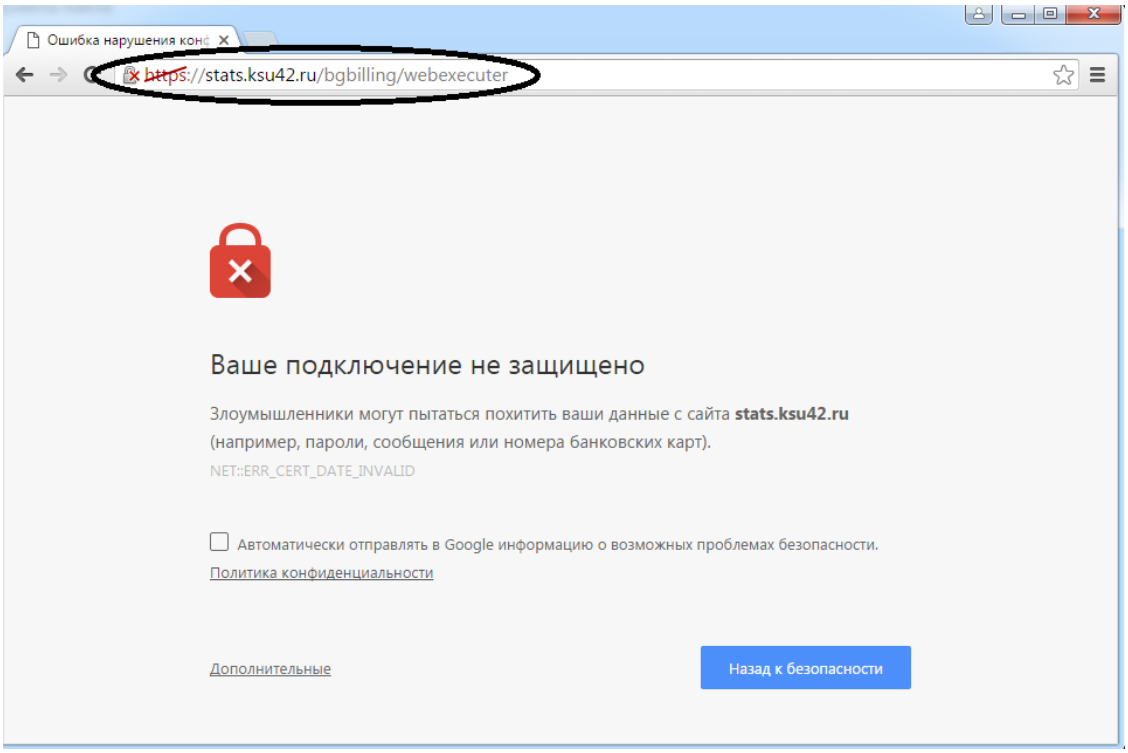

Рисунок 3 – вид адресной строки браузера при недостоверном (просроченном) сертификате SSL

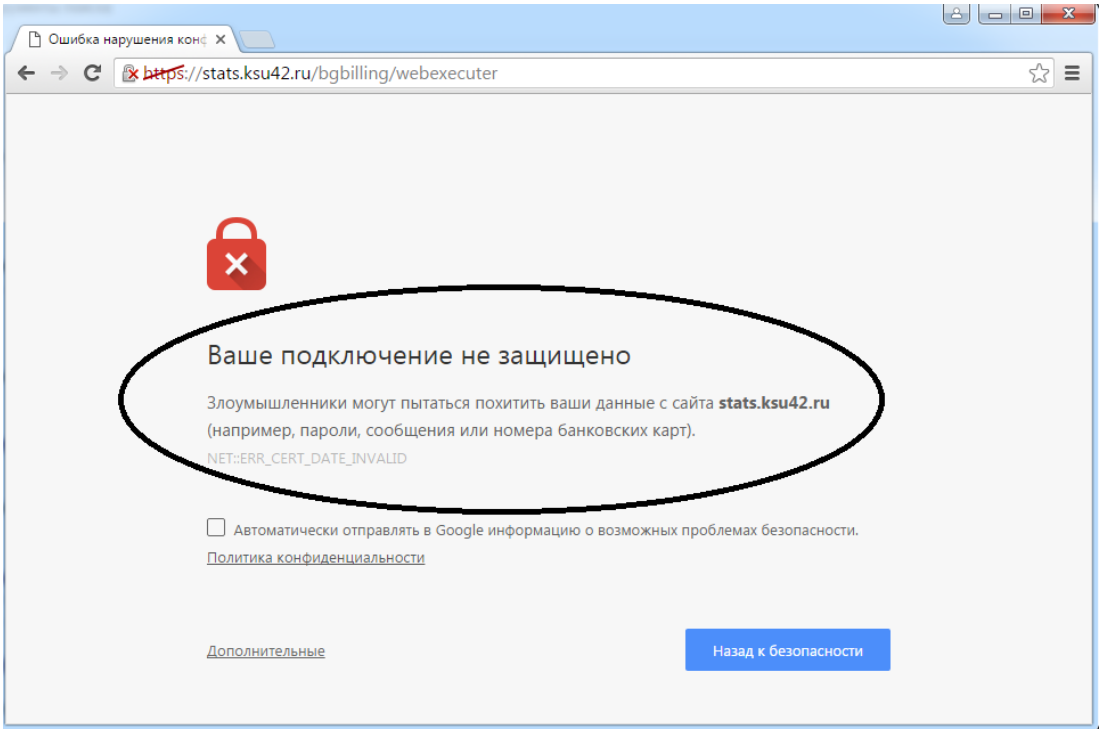

Рисунок 4 – предупреждение браузера при недостоверном (просроченном) сертификате SSL

– не нажимать ("кликать") активные элементы всплывающих окон веб-страниц (сообщения о том, что СВТ заражено или требует оптимизации, сообщение с предложением к знакомству, рекламные сообщения и т.п.)[4];

[4] Всплывающие окна могут содержать в себе ссылку на заранее зараженные Интернет-ресурсы. Например, на экране СВТ пользователя отображается окно с уведомлением о проблеме или необходимости обновления конфигурации СВТ. В этом же окне приводится ссылка на соответствующее обновление или исправление. После загрузки и установки файла сфабрикованная проблема исчезает, и пользователь продолжает работу, не подозревая о том, что он установил вредоносную программу.

– следить за доменными именами интернет-сервисов. Примеры доменных имен: социальная сеть "вконтакте" – vk.com; новостной сайт "Лента" – lenta.ru[5];

– не использовать общедоступные и личные "облачные" сервисы для хранения и обмена служебной информацией (в том числе российского происхождения)[6];

– избегать самостоятельной установки плагинов (расширений, дополнений) к браузерам[7].

4. Правила использования паролей

4.1. Аутентификацию пользователя (ввод пароля) следует использовать во всех информационных системах.

4.2. Следует отказаться от использования функции "запоминания пароля", так как при получении физического доступа к СВТ, любой пользователь может зайти под запомненными учетными данными.

4.3. Рекомендуется для входа в разные информационные системы (например, почтовый сервис и система электронного документооборота) использовать уникальные пароли (отличающиеся друг от друга).

4.4. Рекомендуемые правила создания паролей:

– пароль содержит символы верхнего и нижнего регистров;

– пароль содержит комбинации букв и цифр;

– пароль содержит специальные символы (!@№;%:?*- и т.п.);

– длина пароля составляет не менее 8 символов;

– пароль не несет смысловую нагрузку (например: пароль – "Lj,hj1" в русской раскладке "Добро1"), или не является общераспространенной комбинацией клавиш (например: Qwerty1234; Asdasd123 и т.п.).

Рекомендуется использовать в работе только "сложные" пароли, создаваемые, например, с помощью "парольных фраз"[8].

4.5. Пароль пользователя составляет его личную тайну.

4.6. Ограничения при использовании паролей:

---

[5] Злоумышленником могут создаваться "поддельные" Интернет-ресурсы: например, адрес 0dnoklassniki.ru или vk0ntakte.ru (вместо буквы о – используется цифра 0) не являются реальными адресами социальных сетей. Следует помнить, что внешний вид "поддельных" сайтов может быть максимально приближен к дизайну оригинальных Интернет-ресурсов. Злоумышленник может использовать "поддельные" сайты как для распространения вирусных программ, так и для кражи пользовательских персональных данных пользователей (логин и пароль, номера кредитных карт и т.п.) путем ввода пользователя в заблуждение.

[6] При хранении и обмене служебной информацией на общедоступных и личных "облачных" сервисах к данным имеют доступ посторонние лица (владельцы "облачных" сервисов или производители устройств хранения данных (SAN/NAS).

[7] Плагины взаимодействуют с данными уже после того, как пользователь вошёл в браузер. В этом случае привычные механизмы защиты не эффективны (например, шифрование трафика не обеспечит конфиденциальность данных). История посещений, круг общения, привычки – всё, что "знает" браузер, потенциально доступно коду плагина.

[8] Пароль, образованный из парольной фразы, с несвязанными друг с другом (отсутствие смысловой нагрузки) словами и цифрами: "41 трезвый аллигатор чинит дерево", от каждого слова во фразе берутся первые два символа ("41тралчиде", можно больше) и вводятся в режиме ввода латинских символов – то есть "41nhfkxblt". Дополнительно для усиления пароля можно каждую первую букву каждого слова фразы сделать в верхнем регистре – "41NhFkXbLt".

– использовать служебные пароли в личных целях (например, использовать служебный пароль при регистрации в социальных сетях или общедоступных почтовых сервисах);

– записывать служебные пароли на любых носителях (на бумажных стикерах, в блокнотах, в файлах текстового формата и т.п.), и хранить их в доступном месте (приклеивать на монитор, хранить под клавиатурой, в ежедневнике и т.п.).

5. Правила использования электронной почты

5.1. Довольно часто в почтовый ящик приходят письма с рекламой (так называемый "спам"). Наряду с обычной рекламой, **метод рассылки спама используется злоумышленниками для кражи служебной информации из информационных систем государственных органов.** Основная опасность спам-писем заключается во внедрении вредоносного кода (компьютерного вируса) на персональный компьютер пользователя. Вредоносный код может находиться в теле письма в виде вложения, либо в письме находится гиперссылка на вредоносный код.

5.2. При получении письма следует проверять:

– авторство письма (от кого получено письмо);

– тему письма;

– наличие в письме вложений;

– содержимое письма (информационный текст) на наличие гиперссылок и других активных элементов (картинки, кнопки "нажми сюда", и т.п.).

5.3. Проверка авторства письма.

Автор спама может указать любое имя в адресной строке отправителя (от кого получено письмо). Поэтому следует учитывать, что спам-письмо может быть получено как от незнакомых адресов, так и с адресов, чьи имена максимально похожи с известными.

Примеры:

– письмо пришло с почтового ящика **mike@biz-sell.ru**, имя которого незнакомо и от которого никаких писем не ожидалось;

– письмо пришло с почтового ящика: **a.a.ivanov@kvh.gov.ru**, **a.a.ivanov@khv.gov.com, имя которого максимально приближено (**замаскировано) под легальные адреса Правительства края (реальное имя почтового ящика сотрудника одного из структурных подразделений администрации Губернатора и Правительства края: **a.a.ivanov@khv.gov.ru)**. Также современные технологии позволяют "подменять" адрес отправителя, т.е. он целиком может соответствовать реальному имени почтового ящика сотрудника одного из структурных подразделений администрации Губернатора и Правительства края или органа исполнительной власти края.

Необходимо тщательно проверять адрес отправителя и, в случае сомнения, игнорировать данное письмо.

5.4. Проверка темы письма.

Как правило, в ходе деловой переписки собеседники указывают в поле "тема письма" информацию, наиболее близкую по содержанию тела письма.

Самое распространенное содержание тем спам-писем, рассылаемых злоумышленниками:

– дешевые финансовые предложения (кредиты, ипотеки);

– много восклицательных знаков в заголовке, а также знаки вопроса, сердечки, плюсики;

– риторические вопросы, как в рекламных текстах;

– вопрос, требующий срочного решения;

– денежные суммы, наименование валют в заголовке (100 руб., 5$);

– фрагменты текста, выделенные яркими цветами;

– словосочетания: заработай тут, нажми сюда, бесплатно 1 час, купи здесь, и т.п.;

– секрет моментального успеха;

– гарантия вернуть деньги;

– тема или отдельные слова заглавными буквами;

– в теме слова или словосочетания, связанные с деньгами: "Бесплатно", "Купи", "Заработай", "Скидка", "Деньги", "Распродажа" и т.п.

Например, в теме письма призыв к действию, связанному с получением денег: "Получайте дополнительные 16000 на ваш счет" (рисунок 5).

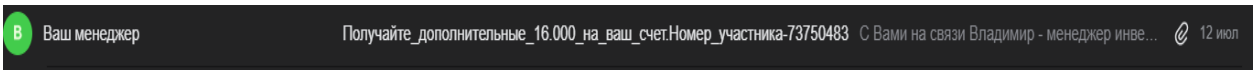

Рисунок 5 – необычная тема письма

5.5. Проверка вложений к письму.

5.5.1. Вредоносный код чаще всего внедряется через прилагаемые к спам письму гиперссылки, вложенные файлы, активные элементы (кнопки, картинки в теле письма и т.п.).

5.5.2. Гиперссылка (обычный вид **http://адрес_сайта.имя_домена**) переводит пользователя на заведомо зараженный Интернет-ресурс.

5.5.3. Вложенный файл может иметь как стандартное расширение (например, *.doc, *.xls, *.rar, *.zip и пр.), так и нестандартное (например, *.zip1).

5.5.4. Имя файла может иметь произвольный вид, начиная от набора символов (например, asdasd.doc), заканчивая именами, завуалированными под документы, создаваемые в органах государственной власти (например: договор на оказание услуг.doc, решение МВК.zip). Например, спам-письмо имеет вложение .eml (рисунок 6).

5.5.5. Расширение файла также может быть "замаскировано" под общепринятые форматы. Например, в исполняемом файле с именем "договор_на_оказание_услуг.doc.scr" расширением является *.scr. При выключенной опции отображения расширений имен файлов в операционной системе зараженное вложение будет иметь привычное имя для файлов Microsoft Word, что увеличивает вероятность запуска файла и дальнейшего заражения.

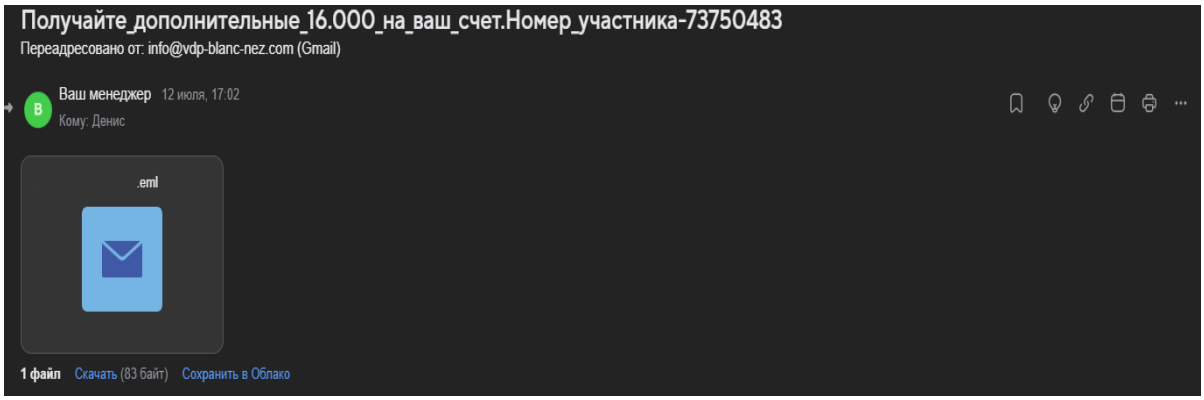

Рисунок 6 – необычные вложения.

5.5.6. Зараженные файлы могут быть получены в социальных сетях или в интернет-мессенджерах, в том числе от учетной записи из списка контактов.

5.5.7. Проверка содержимого письма.

5.5.8. В теле письма могут быть гиперссылки и другие активные элементы (картинки, кнопки "нажми сюда" и т.п.). Настройки по умолчанию почтового сервиса Правительства края (АРМ ГС), работающего через веб-интерфейс (**https://e.armgs.team**) блокируют изображения в письмах. При этом в служебных целях доступна возможность включения пользователем активного содержания письма.

5.5.9. Как показано на рисунке 7, тело письма (информационный текст) содержит вложения, однако на самом деле это гиперссылки на зараженные веб-ресурсы.

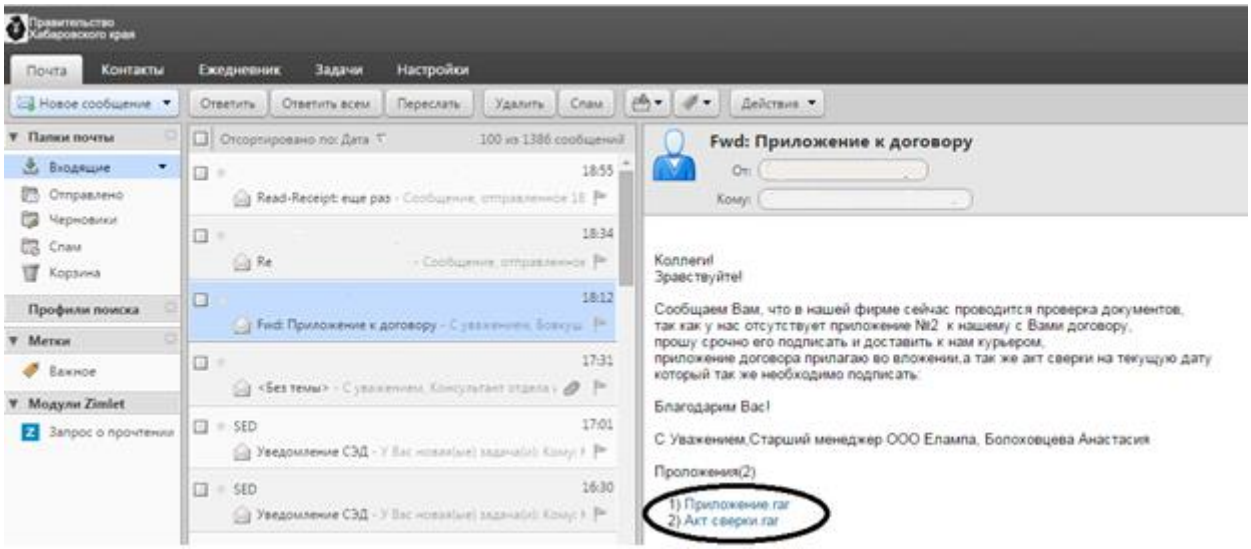

Рисунок 7 – "вложения", которые на самом деле являются гиперссылками.

5.5.10. Вложения в веб-интерфейсе АРМ ГС размещаются не в теле письма, а в специальном поле, как показано на рисунке 8.

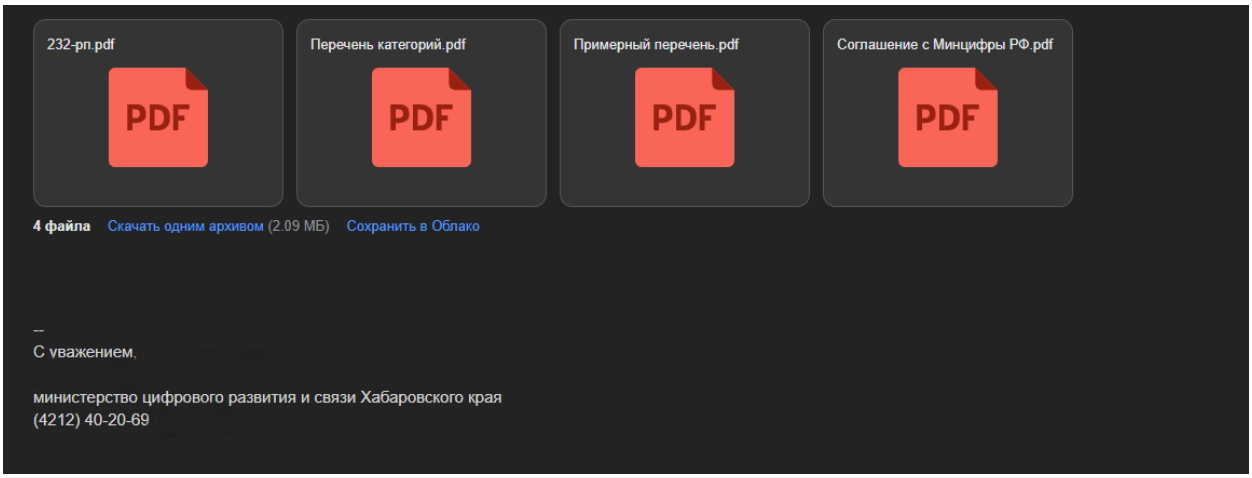

Рисунок 8 – примерный вид легального письма

5.5.11. При подозрении на спам-письмо необходимо обратиться к ответственному за обеспечение безопасности информации.

5.5.12. Нажатие любых активных элементов в полученном письме может повлечь заражение СВТ вирусным программным обеспечением.

5.6. Типовые рекомендации при получении подозрительного письма:

– при получении письма от знакомого адресата с подозрительным содержанием (в особенности, если Вы не ожидали получения писем) необходимо уточнить у адресата факт отправки письма;

– использование правил фильтрации почтовых сообщений в качестве дополнительного метода защиты от спама[9].

5.7. Спам-письма могут быть направлены с целью получения доступа к критическим данным (именам пользователей и паролям). Такой вид мошенничества называется "фишинг". Пример фишингового письма, отправленного с почтового сервиса, запрашивающего "подтверждение авторизации" приведен на рисунке 9. Злоумышленник создает ссылку на заранее подготовленный ресурс, который визуально выглядит аналогично ресурсу, куда пользователь намеревается перейти. После первичного ввода имени учетной записи и пароля, введенные данные записываются на серверах злоумышленника, пользователю выдается сообщение об ошибке ввода и далее следует переадресация на легитимный ресурс.

[9] Перемещение писем от доверенных адресатов в специально созданные в почтовом ящике папки, так называемая фильтрация. Данный механизм позволит защититься от спам-писем от адресатов с именами, замаскированными под легальные. Письмо пришло с почтового ящика: a.a.ivanov@khv.gvo.ru, a.a.ivanov@khv.gov.com, имя которого максимально приближено (замаскировано) под легальные адреса Правительства края (реальное имя почтового ящика сотрудника одного из структурных подразделений администрации Губернатора и Правительства края: a.a.ivanov@khv.gov.ru). Однако данный механизм не защищает от полностью подделанного адреса или при получении письма от легального адресата в случае компрометации пользовательского пароля. Полученное письмо от доверенного адресата, не обработанное заданным правилом фильтрации, будет являться ложным. В таком случае необходимо обратиться к ответственному за обеспечение безопасности информации в ИОК. Производить какие-либо действия с письмом, нажимать любые активные элементы и удалять письмо до проведения разбирательства запрещается.

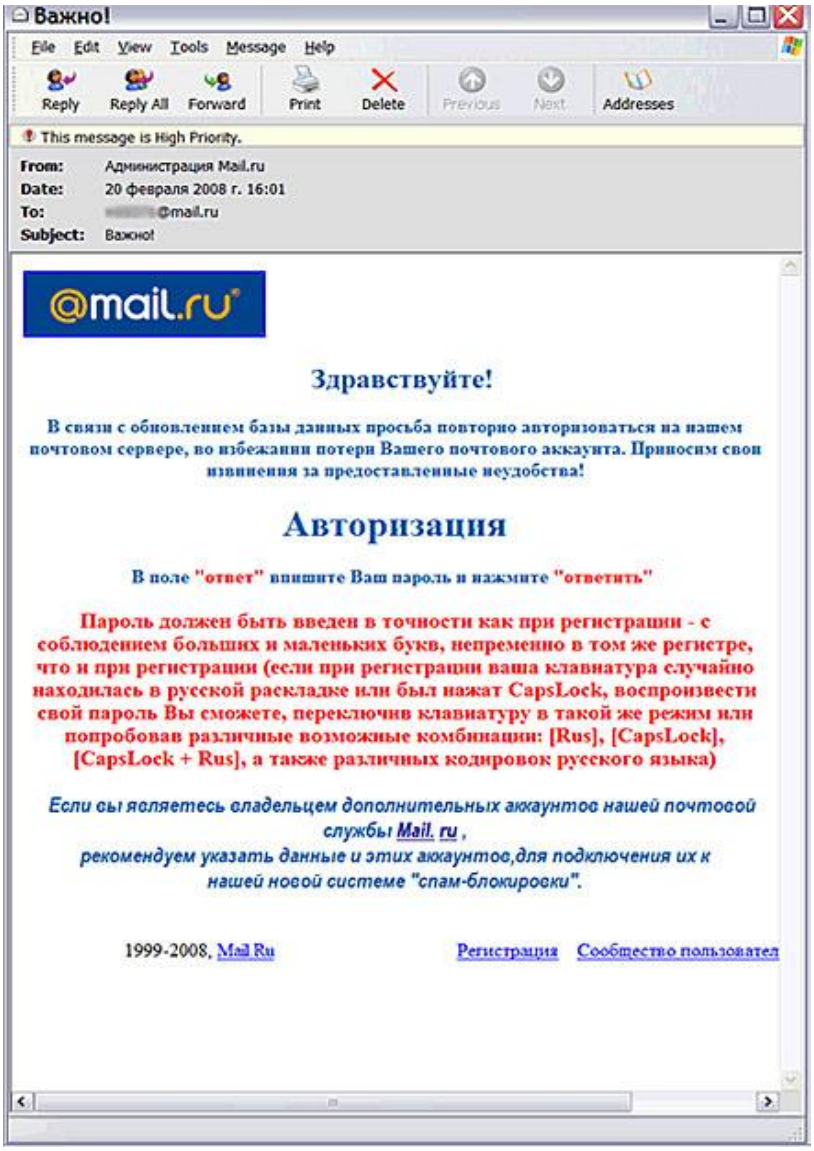

Рисунок 9 – вариант "фишингового" письма.

5.8. Пример типичного спам-письма приведен на рисунке 10. На данном примере видно, что письмо отправлено адресатом с подозрительного почтового ящика (1), имеет вложение (2), тема письма не относится к служебной деятельности органов государственной власти (3), письмо имеет активные элементы (картинка) (4).

5.9. Второй пример спам-письма без указания "якорей", по которым возможно установить принадлежность письма к спаму приведен на рисунке 11.

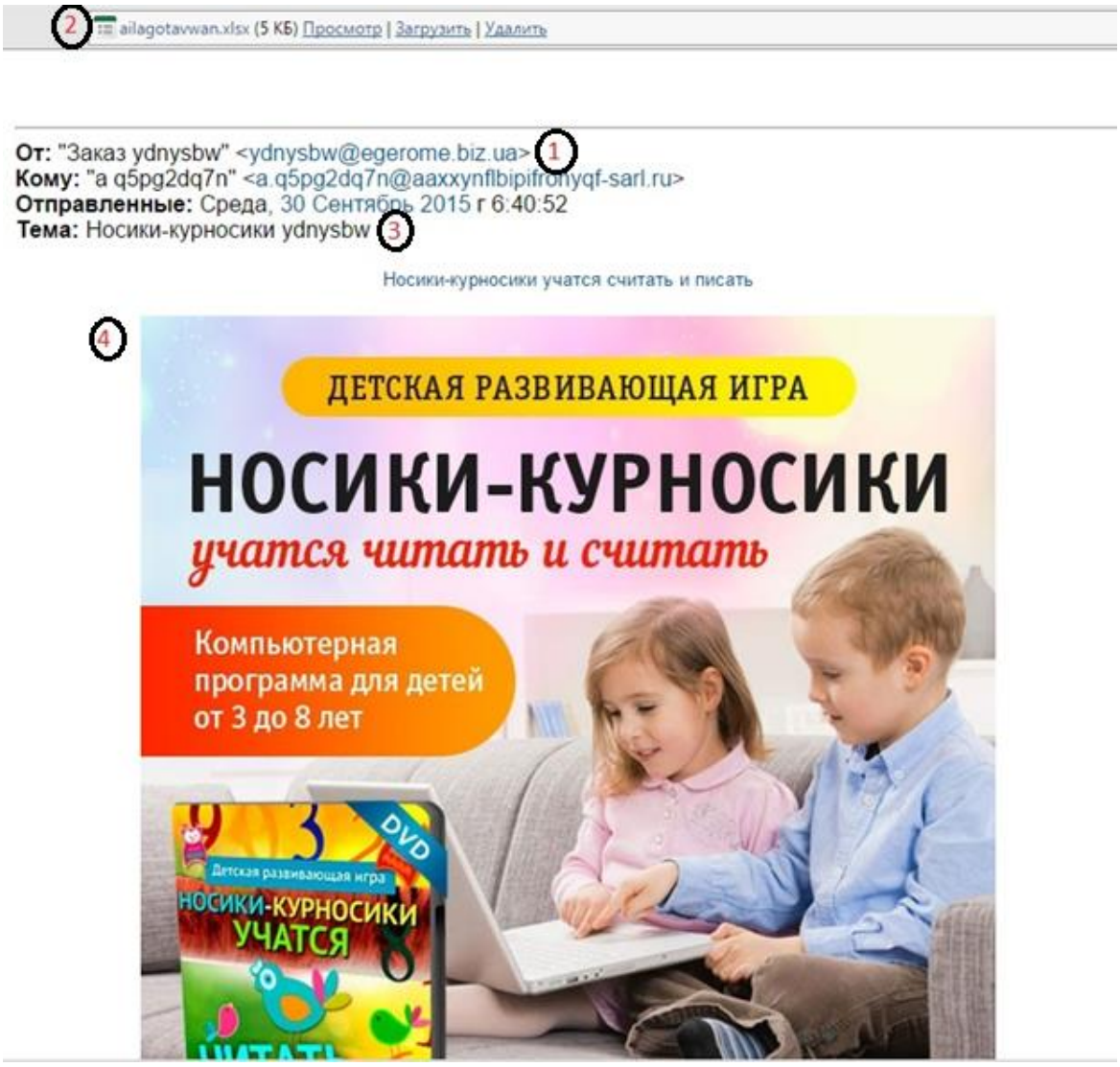

Рисунок 10 – примерный вид типичного спам-письма.

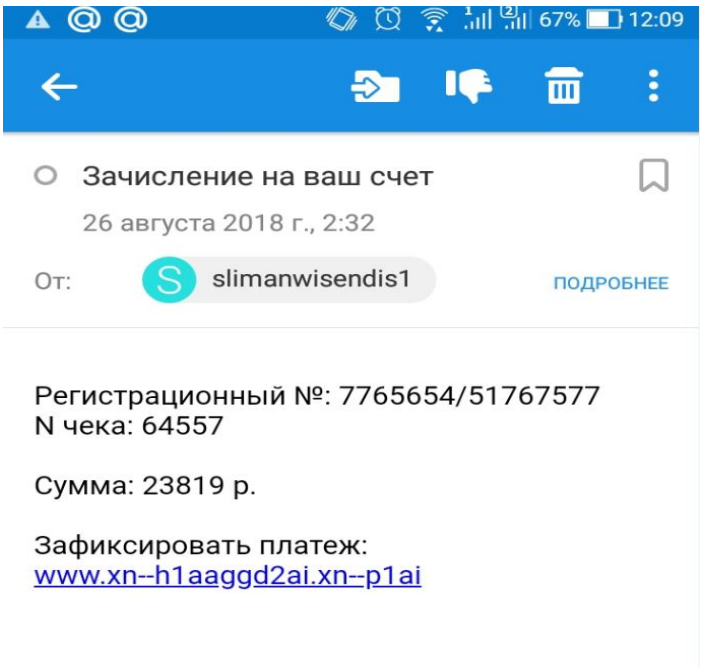

Рисунок 11 – примерный вид типичного спам-письма

5.10. Для уменьшения количества спам-писем не следует использовать свой служебный почтовый адрес на общедоступных интернет-сайтах (при регистрации в социальных сетях, интернет-магазинах, в качестве контактной информации и т.п.).

5.11. Министерство цифрового развития и связи края **НИКОГДА НЕ ЗАПРАШИВАЕТ** у пользователей почтового сервиса Правительства края (АРМ ГС) имена их учетных записей и пароли к ним, не рассылает письма с любым содержанием в отношении запроса учетных данных пользователей или необходимости смены пароля на стороннем ресурсе.

6. Использование средств антивирусной защиты

6.1. При выполнении служебных обязанностей возможно возникновение ситуаций, при которых реакция СВТ на действие пользователей не является ожидаемой.

6.2. Признаки вирусного заражения (без уведомления антивирусного средства):

– невозможность загрузки операционной системы;

– самовольная перезагрузка операционной системы;

– внезапная остановка работы программного обеспечения - "зависание";

– вывод на экран непредусмотренных сообщений, изображений и звуковых сигналов;

– постоянное обращение к жесткому диску при простое компьютера (на системном блоке постоянно горит или мигает его светодиод) вне зависимости от действия или бездействия пользователя;

– вывод на экран предупреждений антивирусного программного обеспечения о попытке несанкционированного выхода в сеть Интернет;

– компьютер работает заметно медленнее обычного;

– самопроизвольный запуск программного обеспечения;

– "зависание" или необычное поведение интернет-браузера (например, подмена одного сайта другим, самопроизвольная подмена "домашней" страницы и/или поискового сайта, невозможность закрыть окно браузера);

– неуправляемая работа подключенных к компьютеру устройств (внезапное открытие или закрытие лотка CD-ROM или DVD-ROM, самопроизвольное движение курсора мыши);

– медленная работа браузера сети Интернет (открытие веб-страниц, просмотр видеофайлов, прослушивание аудиофайлов);

– знакомые говорят о сообщениях от имени пользователя, которые пользователь не отправлял (отправка сообщений в интернет-мессенджерах, электронных писем);

– большое количество сообщений в почтовом ящике без обратного адреса и заголовка;

– отказ работы антивирусного средства;

– самопроизвольное создание файлов на жестком диске компьютера;

– самопроизвольное исчезновение файлов и каталогов или искажение их содержимого;

– предупреждение монитора (антивирусного ПО) об атаке.

Данный перечень не является полным.

6.3. При обнаружении вируса или подозрении на вирусное заражение следует:

– приостановить работу на своем СВТ и возобновлять ее только после удаления вирусной программы и нейтрализации последствий вирусного заражения;

– сообщить ответственному за обеспечение безопасности информации ИОК об обнаруженном вирусе или подозрении на вирусное заражение, и источнику, откуда был получен зараженный файл (владелец), если источник получения имеет высокий уровень доверия (например, коллеги с других ИОК, федеральных ИОК, органов местного самоуправления, организаций, учреждений).

7. Обращение с мобильными устройствами связи (смартфонами, сотовыми телефонами)

7.1. При переписке в интернет-мессенджерах и посредством СМС возможна подмена адресата, поэтому при получении "необычных" сообщений от коллег, в особенности руководителей, следует уточнить действительно ли от них приходило сообщение. "Необычным" сообщением может быть:

– сообщение, содержащее текст, написанный не в обычном стиле адресата. Например, коллега, с которым поддерживаются близкие дружеские отношения, скорее всего, не станет присылать сообщение в сухом официальном стиле, и наоборот;

– сообщение, в котором слишком много грамматических ошибок, хотя легальный автор обычно пишет грамотно, и наоборот;

– сообщение, содержащее неожиданный призыв к определенным действиям. Например, просьба или приказ зайти на веб-ресурс, позвонить по определенным номерам (обычно пишутся в теле сообщения), выслать ту или иную информацию на указываемый адрес (почтовый ящик).

8. Взаимодействие с технической поддержкой

8.1. По вопросам, связанным с работоспособностью СВТ, операционных систем и прикладного программного обеспечения (офисные программы, архиваторы, программы бухгалтерского и кадрового учета и т.п.), средств защиты информации, следует обращаться только в службу технической поддержки (ответственному за информационную безопасность в ИОК). Основные правила при взаимодействии:

– первичное обращение в службу поддержки всегда исходит от пользователя (телефонный звонок или электронная заявка). Если звонит специалист службы поддержки, следует убедиться, что он является тем, кем

он себя называет (например, позвонить в службу технической поддержки и уточнить контактную информацию о звонившем сотруднике и его задании)[10].

– специалист службы поддержки (ответственный за обеспечение безопасности в ИОК) не запрашивает у пользователя парольную информацию. Сообщать личный пароль специалисту службы поддержки не допускается. Так же специалист технической поддержки никогда не должен просить пользователя зарегистрироваться, где бы то ни было, чтобы затем сообщить ему пароль.

8.2. При общении со службой технической поддержки необходимо быть вежливым и соблюдать этикет. Грубые и резкие высказывания, требования и угрозы исключаются.

8.3. При попытке запугивания со стороны специалиста технической поддержки необходимо:

– вежливо попросить внятно представиться (фамилия, имя, отчество), назвать должность и место работы;

– не передавая никаких запрашиваемых сведений, сообщить о звонке своему непосредственному руководителю и ответственному за обеспечение безопасности информации в ИОК.

Контактная информация:

Отдел информационной безопасности управления мультимедийных и специальных информационных технологий министерства цифрового развития и связи края, тел. (4212) 40-20-68, e-mail: ib@khv.gov.ru

[10] Возможный случай, при котором специалист службы поддержки звонит пользователю – это работа по заявке, уточнение проблемы и т.п. либо оценка удовлетворенности пользователя по решению технической проблемы, для закрытия заявки.

Приложение №1 к Методическим рекомендациям по использованию информационно-коммуникационных технологий, созданию, развитию, модернизации, эксплуатации информационных систем и информационно-телекоммуникационных инфраструктуры

Примерный алгоритм действий в случае получения подозрительного письма