[ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ](https://revda-ds17.ru/index.php/bezopasnost-v-ou/informatsionnaya-bezopasnot/pedagogicheskim-rabotnikam/53-informatsionnaya-bezopasnost-dlya-pedagogicheskikh-rabotnikov)

Об­ра­зо­ва­тель­ный про­цесс ка­са­ет­ся наи­ме­нее за­щи­щен­ных от про­па­ган­ды чле­нов об­ще­ства – де­тей и под­рост­ков. В свя­зи с этим си­сте­ма ин­фор­ма­ци­он­ной без­опас­но­сти об­ра­зо­ва­тель­ной ор­га­ни­за­ции долж­на не толь­ко обес­пе­чи­вать со­хран­ность баз дан­ных и со­дер­жа­щих­ся в них мас­си­вов кон­фи­ден­ци­аль­ных све­де­ний, но и га­ран­ти­ро­вать невоз­мож­ность до­сту­па в сте­ны кол­ле­джа лю­бой про­па­ган­ды, как неза­кон­но­го ха­рак­те­ра, так и без­обид­ной, но пред­по­ла­га­ю­щей воз­дей­ствие на со­зна­ние уча­щих­ся в за­ве­де­ни­ях сред­не­го про­фес­сио­наль­но­го об­ра­зо­ва­ния.

Пе­да­го­ги­че­ско­му ра­бот­ни­ку крайне важ­но иметь на­вы­ки ме­диа­гра­мот­но­сти и «ин­фор­ма­ци­он­ной ги­ги­е­ны», уметь ра­бо­тать с совре­мен­ным про­грамм­ным обес­пе­че­ни­ем, знать ос­нов­ные ас­пек­ты ин­фор­ма­ци­он­ной без­опас­но­сти, а так­же при­ме­нять ука­зан­ные на­вы­ки не толь­ко в по­все­днев­ной жиз­ни, но и в об­ра­зо­ва­тель­ном про­цес­се. Ин­фор­ма­ци­он­ная без­опас­ность об­ра­зо­ва­тель­ной ор­га­ни­за­ции вклю­ча­ет си­сте­му мер, на­прав­лен­ных на за­щи­ту ин­фор­ма­ци­он­но­го про­стран­ства и пер­со­наль­ных дан­ных от слу­чай­но­го или на­ме­рен­но­го про­ник­но­ве­ния с це­лью хи­ще­ния ка­кой-ли­бо ин­фор­ма­ции или вне­се­ния из­ме­не­ний в кон­фи­гу­ра­цию си­сте­мы. Вто­рым ас­пек­том дан­но­го по­ня­тия яв­ля­ет­ся за­щи­та об­ра­зо­ва­тель­но­го про­цес­са от лю­бых све­де­ний, но­ся­щих ха­рак­тер за­пре­щен­ной за­ко­ном про­па­ган­ды, или лю­бых ви­дов ре­кла­мы.

В со­ста­ве мас­си­вов охра­ня­е­мой за­ко­ном ин­фор­ма­ции, на­хо­дя­щей­ся в рас­по­ря­же­нии об­ра­зо­ва­тель­ной ор­га­ни­за­ции, мож­но вы­де­лить три груп­пы:

* пер­со­наль­ные све­де­ния, ка­са­ю­щи­е­ся обу­ча­ю­щих­ся и пре­по­да­ва­те­лей, оциф­ро­ван­ные ар­хи­вы;
* ноу-хау об­ра­зо­ва­тель­но­го про­цес­са, но­ся­щие ха­рак­тер ин­тел­лек­ту­аль­ной соб­ствен­но­сти и за­щи­щен­ные за­ко­ном;
* струк­ту­ри­ро­ван­ная учеб­ная ин­фор­ма­ция, обес­пе­чи­ва­ю­щая об­ра­зо­ва­тель­ный про­цесс (биб­лио­те­ки, ба­зы дан­ных, обу­ча­ю­щие про­грам­мы).

Все эти све­де­ния мо­гут стать не толь­ко объ­ек­том хи­ще­ния. На­ме­рен­ное про­ник­но­ве­ние в них мо­жет на­ру­шить со­хран­ность оциф­ро­ван­ных книг, уни­что­жить хра­ни­ли­ща зна­ний, вне­сти из­ме­не­ния в код про­грамм, ис­поль­зу­е­мых для обу­че­ния.

Обя­зан­но­стя­ми лиц, от­вет­ствен­ных за за­щи­ту ин­фор­ма­ции, долж­но стать со­хра­не­ние дан­ных в це­лост­но­сти и непри­кос­но­вен­но­сти и обес­пе­че­ние их:

* до­ступ­но­сти в лю­бое вре­мя для лю­бо­го ав­то­ри­зи­ро­ван­но­го поль­зо­ва­те­ля;
* за­щи­ты от лю­бой утра­ты или вне­се­ния несанк­ци­о­ни­ро­ван­ных из­ме­не­ний;
* кон­фи­ден­ци­аль­но­сти, недо­ступ­но­сти для тре­тьих лиц.

Осо­бен­но­стью угроз ста­но­вит­ся не толь­ко воз­мож­ность хи­ще­ния све­де­ний или по­вре­жде­ние мас­си­вов ка­ки­ми-ли­бо со­зна­тель­но дей­ству­ю­щи­ми ха­кер­ски­ми груп­пи­ров­ка­ми, но и са­ма де­я­тель­ность под­рост­ков, на­ме­рен­но, по зло­му умыс­лу или оши­боч­но спо­соб­ных по­вре­дить ком­пью­тер­ное обо­ру­до­ва­ние или вне­сти ви­рус. Вы­де­ля­ют­ся пять групп объ­ек­тов, ко­то­рые мо­гут под­верг­нуть­ся на­ме­рен­но­му или нена­ме­рен­но­му воз­дей­ствию:

1. ком­пью­тер­ная тех­ни­ка и дру­гие ап­па­рат­ные сред­ства, ко­то­рые мо­гут быть по­вре­жде­ны в ре­зуль­та­те ме­ха­ни­че­ско­го воз­дей­ствия, ви­ру­сов, а так­же по иным при­чи­нам;
2. про­грам­мы, ис­поль­зу­е­мые для обес­пе­че­ния ра­бо­то­спо­соб­но­сти си­сте­мы или в об­ра­зо­ва­тель­ном про­цес­се, ко­то­рые мо­гут по­стра­дать от ви­ру­сов или ха­кер­ских атак;
3. дан­ные, хра­ни­мые как на жест­ких дис­ках, так и на от­дель­ных но­си­те­лях;
4. сам пер­со­нал, от­ве­ча­ю­щий за ра­бо­то­спо­соб­ность ин­фор­ма­ци­он­ных си­стем;
5. обу­ча­ю­щи­е­ся, под­вер­жен­ные внеш­не­му агрес­сив­но­му ин­фор­ма­ци­он­но­му вли­я­нию.

Угро­зы, на­прав­лен­ные на по­вре­жде­ние лю­бо­го из ком­по­нен­тов си­сте­мы, мо­гут но­сить как слу­чай­ный, так и осо­знан­ный пред­на­ме­рен­ный ха­рак­тер. Сре­ди угроз, не за­ви­ся­щих от на­ме­ре­ния пер­со­на­ла, обу­ча­ю­щих­ся или тре­тьих лиц, мож­но на­звать:

* лю­бые ава­рий­ные си­ту­а­ции, на­при­мер, от­клю­че­ние элек­тро­энер­гии или за­топ­ле­ние;
* ошиб­ки пер­со­на­ла;
* сбои в ра­бо­те про­грамм­но­го обес­пе­че­ния;
* вы­ход тех­ни­ки из строя;
* про­бле­мы в ра­бо­те си­стем свя­зи.

Все эти угро­зы ин­фор­ма­ци­он­ной без­опас­но­сти но­сят вре­мен­ный ха­рак­тер, пред­ска­зу­е­мы и лег­ко устра­ня­ют­ся дей­стви­я­ми со­труд­ни­ков и спе­ци­аль­ных служб.

На­ме­рен­ные угро­зы ин­фор­ма­ци­он­ной без­опас­но­сти но­сят бо­лее опас­ный ха­рак­тер и в боль­шин­стве слу­ча­ев не мо­гут быть пред­ви­де­ны. Их ви­нов­ни­ка­ми мо­гут ока­зать­ся обу­ча­ю­щи­е­ся, со­труд­ни­ки, тре­тьи ли­ца, име­ю­щие умы­сел на со­вер­ше­ние ки­бер­пре­ступ­ле­ния. Для под­ры­ва ин­фор­ма­ци­он­ной без­опас­но­сти та­кое ли­цо долж­но иметь вы­со­кую ква­ли­фи­ка­цию в от­но­ше­нии прин­ци­пов ра­бо­ты ком­пью­тер­ных си­стем и про­грамм. Наи­боль­шей опас­но­сти под­вер­га­ют­ся ком­пью­тер­ные се­ти, ком­по­нен­ты ко­то­рых рас­по­ло­же­ны от­дель­но друг от дру­га в про­стран­стве. На­ру­ше­ние свя­зи меж­ду ком­по­нен­та­ми си­сте­мы мо­жет при­ве­сти к пол­но­му под­ры­ву ее ра­бо­то­спо­соб­но­сти. Важ­ной про­бле­мой мо­жет стать на­ру­ше­ние ав­тор­ских прав, на­ме­рен­ное хи­ще­ние чу­жих раз­ра­бо­ток. Ком­пью­тер­ные се­ти ред­ко под­вер­га­ют­ся внеш­ним ата­кам с це­лью воз­дей­ствия на со­зна­ние де­тей, но и это не ис­клю­че­но. Са­мой се­рьез­ной опас­но­стью в по­доб­ном слу­чае станет ис­поль­зо­ва­ние обо­ру­до­ва­ния об­ра­зо­ва­тель­ной ор­га­ни­за­ции для во­вле­че­ния ре­бен­ка в со­вер­ше­ние пре­ступ­ле­ний экс­тре­мист­ской и тер­ро­ри­сти­че­ской на­прав­лен­но­сти.

С точ­ки зре­ния про­ник­но­ве­ния в пе­ри­метр ин­фор­ма­ци­он­ной без­опас­но­сти и для со­вер­ше­ния хи­ще­ния ин­фор­ма­ции или со­зда­ния на­ру­ше­ния в ра­бо­те си­стем необ­хо­дим несанк­ци­о­ни­ро­ван­ный до­ступ.

Мож­но вы­де­лить несколь­ко ви­дов несанк­ци­о­ни­ро­ван­но­го до­сту­па:

1. Че­ло­ве­че­ский. Ин­фор­ма­ция мо­жет быть по­хи­ще­на пу­тем ко­пи­ро­ва­ния на вре­мен­ные но­си­те­ли, пе­ре­прав­ле­на по элек­трон­ной по­чте. Кро­ме то­го, при на­ли­чии до­сту­па к сер­ве­ру из­ме­не­ния в ба­зы дан­ных мо­гут быть вне­се­ны вруч­ную.
2. Про­грамм­ный. Для хи­ще­ний све­де­ний ис­поль­зу­ют­ся спе­ци­аль­ные про­грам­мы, ко­то­рые обес­пе­чи­ва­ют ко­пи­ро­ва­ние па­ро­лей, ко­пи­ро­ва­ние и пе­ре­хват ин­фор­ма­ции, пе­ре­на­прав­ле­ние тра­фи­ка, де­шиф­ров­ку, вне­се­ние из­ме­не­ний в ра­бо­ту иных про­грамм.
3. Ап­па­рат­ный. Он свя­зан или с ис­поль­зо­ва­ни­ем спе­ци­аль­ных тех­ни­че­ских средств, или с пе­ре­хва­том элек­тро­маг­нит­но­го из­лу­че­ния по раз­лич­ным ка­на­лам, вклю­чая те­ле­фон­ные.

Борь­ба с раз­лич­ны­ми ви­да­ми атак на ин­фор­ма­ци­он­ную без­опас­ность долж­на ве­стись на пя­ти уров­нях, при­чем ра­бо­та долж­на но­сить ком­плекс­ный ха­рак­тер. Су­ще­ству­ет ряд ме­то­ди­че­ских раз­ра­бо­ток, ко­то­рые поз­во­лят по­стро­ить за­щи­ту об­ра­зо­ва­тель­ной ор­га­ни­за­ции на необ­хо­ди­мом уровне.

Ука­зом Пре­зи­ден­та Рос­сий­ской Фе­де­ра­ции от 1 июня 2012г. №761 утвер­жде­на На­цио­наль­ная стра­те­гия дей­ствий в ин­те­ре­сах де­тей, опре­де­ля­ю­щая сте­пень угроз и ме­ры за­щи­ты их без­опас­но­сти. Дей­ствия по огра­ни­че­нию агрес­сив­но­го воз­дей­ствия на со­зна­ние ре­бен­ка долж­ны стать ос­нов­ны­ми. На вто­ром ме­сте долж­но ока­зать­ся обес­пе­че­ние без­опас­но­сти баз дан­ных.

За­щи­та ин­фор­ма­ции опи­ра­ет­ся на дей­ству­ю­щие в этой сфе­ре нор­ма­тив­ные пра­во­вые ак­ты, опре­де­ля­ю­щие от­дель­ные ее мас­си­вы как под­ле­жа­щие за­щи­те. Они вы­де­ля­ют те све­де­ния, ко­то­рые долж­ны быть недо­ступ­ны тре­тьим ли­цам по раз­ным при­чи­нам (кон­фи­ден­ци­аль­ная ин­фор­ма­ция, пер­со­наль­ные дан­ные, ком­мер­че­ская, слу­жеб­ная или про­фес­сио­наль­ная тай­на). По­ря­док за­щи­ты пер­со­наль­ных дан­ных опре­де­ля­ет­ся Граж­дан­ским ко­дек­сом Рос­сий­ской Фе­де­ра­ции, Тру­до­вым ко­дек­сом Рос­сий­ской Фе­де­ра­ции, фе­де­раль­ны­ми за­ко­на­ми «Об ин­фор­ма­ции, ин­фор­ма­ци­он­ных тех­но­ло­ги­ях и о за­щи­те ин­фор­ма­ции» и «О пер­со­наль­ных дан­ных». На ос­но­ва­нии дан­ных за­ко­но­да­тель­ных ак­тов раз­ра­ба­ты­ва­ют­ся ме­то­ди­ки для обес­пе­че­ния за­щи­ты ин­фор­ма­ции.

Пе­да­го­ги­че­ским ра­бот­ни­кам необ­хо­ди­мо пом­нить, что в об­ра­зо­ва­тель­ной сфе­ре боль­шую роль иг­ра­ет си­сте­ма мо­раль­но-эти­че­ских цен­но­стей. На ней долж­на ос­но­вы­вать­ся си­сте­ма мер, за­щи­ща­ю­щих под­рост­ка от трав­ми­ру­ю­щей, эти­че­ски некор­рект­ной, неза­кон­ной ин­фор­ма­ции. В це­лях за­щи­ты от про­па­ган­ды необ­хо­ди­мо при­ме­нять нор­мы фе­де­раль­ных за­ко­нов «О за­щи­те де­тей от ин­фор­ма­ции, при­чи­ня­ю­щей вред их здо­ро­вью и раз­ви­тию», «Об ос­нов­ных га­ран­ти­ях прав ре­бен­ка в Рос­сий­ской Фе­де­ра­ции» и За­ко­на Туль­ской об­ла­сти «О за­щи­те прав ре­бен­ка», опре­де­ля­ю­щие пра­ва несо­вер­шен­но­лет­них на за­щи­ту от све­де­ний, при­чи­ня­ю­щих вред здо­ро­вью и (или) раз­ви­тию де­тей. К та­ким све­де­ни­ям от­но­сит­ся ин­фор­ма­ция:

* по­буж­да­ю­щая де­тей к со­вер­ше­нию дей­ствий, пред­став­ля­ю­щих угро­зу их жиз­ни и (или) здо­ро­вью, в том чис­ле к при­чи­не­нию вре­да сво­е­му здо­ро­вью, са­мо­убий­ству;
* спо­соб­ная вы­звать у де­тей же­ла­ние упо­тре­бить нар­ко­ти­че­ские сред­ства, пси­хо­троп­ные и (или) одур­ма­ни­ва­ю­щие ве­ще­ства, та­бач­ные из­де­лия, ал­ко­голь­ную и спир­то­со­дер­жа­щую про­дук­цию, при­нять уча­стие в азарт­ных иг­рах, за­ни­мать­ся про­сти­ту­ци­ей, бро­дяж­ни­че­ством или по­про­шай­ни­че­ством;
* обос­но­вы­ва­ю­щая или оправ­ды­ва­ю­щая до­пу­сти­мость на­си­лия и (или) же­сто­ко­сти ли­бо по­буж­да­ю­щая осу­ществ­лять на­силь­ствен­ные дей­ствия по от­но­ше­нию к лю­дям или жи­вот­ным;
* от­ри­ца­ю­щая се­мей­ные цен­но­сти, про­па­ган­ди­ру­ю­щая нетра­ди­ци­он­ные сек­су­аль­ные от­но­ше­ния и фор­ми­ру­ю­щая неува­же­ние к ро­ди­те­лям и (или) дру­гим чле­нам се­мьи;
* оправ­ды­ва­ю­щая про­ти­во­прав­ное по­ве­де­ние;
* со­дер­жа­щая нецен­зур­ную брань;
* со­дер­жа­щая ин­фор­ма­цию пор­но­гра­фи­че­ско­го ха­рак­те­ра;
* пред­став­ля­е­мая в ви­де изоб­ра­же­ния или опи­са­ния же­сто­ко­сти, физи­че­ско­го и (или) пси­хи­че­ско­го на­си­лия, пре­ступ­ле­ния или ино­го ан­ти­об­ще­ствен­но­го дей­ствия;
* вы­зы­ва­ю­щая у де­тей страх, ужас или па­ни­ку, в том чис­ле пред­став­ля­е­мая в ви­де изоб­ра­же­ния или опи­са­ния в уни­жа­ю­щей че­ло­ве­че­ское до­сто­ин­ство фор­ме нена­силь­ствен­ной смер­ти, за­боле­ва­ния, са­мо­убий­ства, несчаст­но­го слу­чая, ава­рии или ка­та­стро­фы и (или) их по­след­ствий.

Пе­да­го­ги­че­ско­му кол­лек­ти­ву необ­хо­ди­мо ре­гу­ляр­но при­ни­мать ме­ры по предот­вра­ще­нию рас­про­стра­не­ния в кол­ле­дже ин­фор­ма­ции, ко­то­рая мо­жет трав­ми­ро­вать пси­хи­ку де­тей. Это станет од­ной из ос­нов ин­фор­ма­ци­он­ной без­опас­но­сти. Ука­зан­ный ком­плекс мер це­ли­ком по­стро­ен на со­зда­нии внут­рен­них пра­вил и ре­гла­мен­тов, опре­де­ля­ю­щих по­ря­док ра­бо­ты с ин­фор­ма­ци­ей и ее но­си­те­ля­ми. Это внут­рен­ние ме­то­ди­ки, по­свя­щен­ные ин­фор­ма­ци­он­ной без­опас­но­сти, долж­ност­ные ин­струк­ции, пе­реч­ни све­де­ний, не под­ле­жа­щих пе­ре­да­че. До­пол­ни­тель­но дол­жен быть раз­ра­бо­тан ре­гла­мент, опре­де­ля­ю­щий по­ря­док вза­и­мо­дей­ствия с ком­пе­тент­ны­ми ор­га­на­ми по за­про­сам о предо­став­ле­нии им тех или иных дан­ных и до­ку­мен­тов.

Кро­ме то­го, эти ме­то­ди­ки долж­ны опре­де­лять по­ря­док до­сту­па де­тей к се­ти Ин­тернет в ком­пью­тер­ных клас­сах, воз­мож­ность за­щи­ты неко­то­рых ре­сур­сов неод­но­знач­но­го ха­рак­те­ра от до­сту­па ре­бен­ка, за­прет на поль­зо­ва­ние соб­ствен­ны­ми но­си­те­ля­ми ин­фор­ма­ции. Кро­ме то­го, в об­ра­зо­ва­тель­ной ор­га­ни­за­ции долж­но быть преду­смот­ре­но ис­поль­зо­ва­ние си­сте­мы ро­ди­тель­ско­го кон­тро­ля над ре­сур­са­ми се­ти Ин­тернет. За дан­ную си­сте­му мер и ее внед­ре­ние долж­но от­ве­чать ру­ко­вод­ство об­ра­зо­ва­тель­ной ор­га­ни­за­ции и со­труд­ни­ки со­от­вет­ству­ю­щих ИКТ-под­раз­де­ле­ний.

Важ­но пом­нить, что элек­трон­ная поч­та, к ко­то­рой име­ют до­ступ со­труд­ни­ки и уча­щи­е­ся, долж­на быть кон­тро­ли­ру­е­ма. Оп­ти­маль­но так­же вве­сти пол­ный за­прет на ко­пи­ро­ва­ние лю­бой ин­фор­ма­ции с жест­ких дис­ков ком­пью­те­ров об­ра­зо­ва­тель­ной ор­га­ни­за­ции. Кро­ме то­го, долж­но быть преду­смот­ре­но про­грамм­ное обес­пе­че­ние, огра­ни­чи­ва­ю­щее до­ступ ре­бен­ка на опре­де­лен­ные сай­ты (кон­тент-филь­тры).

Все пе­ре­чис­лен­ные ме­ры долж­ны при­ме­нять­ся в ком­плек­се, при этом необ­хо­ди­мо опре­де­ле­ние од­но­го или несколь­ких лиц, от­ве­ча­ю­щих за ре­а­ли­за­цию всех ас­пек­тов ин­фор­ма­ци­он­ной без­опас­но­сти. Же­ла­тель­но при­вле­че­ние к этой про­бле­ме ро­ди­те­лей (за­кон­ных пред­ста­ви­те­лей) сту­ден­тов, ведь в ря­де слу­ча­ев они по­мо­гут про­ве­сти аудит мер без­опас­но­сти и по­ре­ко­мен­до­вать совре­мен­ные ре­ше­ния. Кро­ме то­го, на ро­ди­те­лей (за­кон­ных пред­ста­ви­те­лей) долж­ны быть воз­ло­же­ны обя­зан­но­сти и по огра­ни­че­нию ин­фор­ма­ции, ко­то­рую ре­бе­нок мо­жет по­лу­чить до­ма. Необ­хо­ди­мо про­смат­ри­вать стра­ни­цы, по­се­ща­е­мые ре­бен­ком. На ос­но­ва­нии ана­ли­за его по­ис­ка мож­но вно­сить из­ме­не­ния в пе­ре­чень сай­тов, до­ступ к ко­то­рым огра­ни­чен с ком­пью­те­ров, уста­нов­лен­ных в учеб­ном за­ве­де­нии.

Ре­а­ли­за­ция ком­плек­са пе­ре­чис­лен­ных мер поз­во­лит обес­пе­чить ин­фор­ма­ци­он­ную без­опас­ность об­ра­зо­ва­тель­но­го про­цес­са, со­хра­нить здо­ро­вье обу­ча­ю­щих­ся и га­ран­ти­ро­вать их гар­мо­нич­ное ду­хов­но-нрав­ствен­ное вос­пи­та­ние.