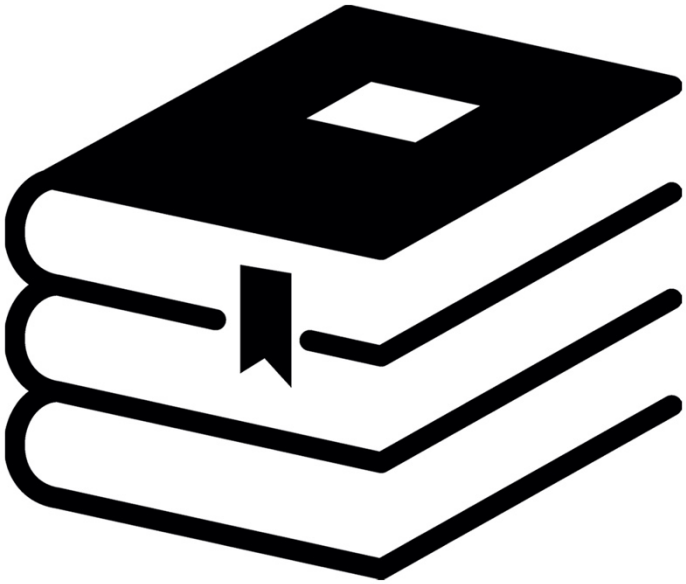
Электронный журнал центра публикаций ПубліЦентр — PubliCentr.ru



ПубліЦентр

Выпуск №5

Липецк - 2022

Педагогический электронный журнал издаётся по решению редакционного совета Всероссийского СМИ ПубліЦентр

Главный редактор сетевого издания
М.Ю. Мальцев

ПубліЦентр. – Вып.5. – Липецк, 2022. – 14 с. с илл.

Авторские материалы, включенные в настоящий электронный журнал, содержат работы, которые помогут педагогам в их профессиональной деятельности. Журнал адресован работникам всех образовательных учреждений Российской Федерации.

www.publicentr.ru | info@publicentr.ru

Об издании ПублиЦентр

www.publicentr.ru

Центр публикаций ПублиЦентр зарегистрирован в качестве образовательного издания. Мы постарались сделать наш основной продукт, электронный журнал, максимально удобным для чтения. Уверены, что вы сразу обратили внимание на дизайн журнала, крупный шрифт и оттенки серого в его оформлении. Такой стиль, на наш взгляд, является оптимальным для комфортного ознакомления с опубликованными материалами. Основная цель нашей деятельности — повышение качества образовательных услуг, а также оказание технической помощи работникам образовательных учреждений Российской Федерации. Специализация издания ПублиЦентр — профессиональные публикации и рецензии. Мы оперативно публикуем материалы, подготавливаем на них рецензии и заверяем всё официальными документами, получить которые можно как в электронном виде, так и на бумажном носителе.

С уважением, редакция издания ПублиЦентр

СОДЕРЖАНИЕ

Автор: Кисткин Алексей Валерьевич

Должность: магистрант

Образовательное учреждение: Пензенский Государственный Университет

Населённый пункт: Пенза, Пензенская область

Тема: Субъективные признаки преступлений в сфере компьютерной информации.

Раздел образования: Организация дополнительного профессионального образования

АННОТАЦИЯ

Дана подробная характеристика субъективных признаков преступлений в сфере компьютерной информации. Сформулированы требования, подпадающие под субъективные признаки привлечения лица к уголовной ответственности за деяние, инкриминируемое в сфере компьютерной информации.

Ключевые слова: преступления в сфере компьютерной информации; субъективные признаки; субъект; вина; цель; мотив.

По официальным данным в России в январе-декабре 2021 года зарегистрировано 517,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,4% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,0% в январе-декабре 2020 года до 25,8%[1].

Оценка криминогенной обстановки преступлений в сфере компьютерной информации дает основания к принятию решительных мер по стороны правоохранителей всего мира с целью ее улучшение,

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/28021552/(дата обращения: 03.03.2022).

уменьшение риска для рядовых граждан попасть в ловушку киберпреступников.

Статистические данные свидетельствуют о достаточно высоком проценте таких правонарушений в общем спектре преступности, а их количество, как и сложность, целенаправленно продвигаются вперед.

Вопросы противодействия преступлений в сфере компьютерной информации на мировом уровне является объектом внимания значительной части ученых и практиков, среди которых можно выделить отечественных специалистов.

По нашему мнению, несмотря на теоретическую и практическую значимость проведенных и опубликованных исследований, затронутая тема исследования имеет еще больше вопросов, как со стороны теоретиков, так и со стороны практиков.

Диспозиция ст. 272 УК РФ не содержит в себе указания на форму вины, однако в данном случае с уверенностью можно говорить об умысле (прямом или косвенном). В случае совершения данного преступления лицо осознает, что его действия носят неправомерный характер, предвидит или может предвидеть наступления общественно опасных последствий, но при этом допускает их наступление.

Неправомерный доступ к компьютерной информации – умышленное деяние, поскольку в диспозиции ст. 272 УК РФ не указано обратное[2].

По общему правилу, ответственность за совершение преступлений, предусмотренных ст. 272 УК РФ наступает с 16 лет, однако ч. 3 ст. 272 предусматривает наличие специального субъекта, совершившего данное преступление[3].

В преступлении, предусмотренном ст. 272 УК РФ, неправомерный доступ к компьютерной информации осуществляется следующими лицами:

1) не имеющими права на доступ к компьютерной информации в данных условиях места и времени, но осуществляющими «неправомерный доступ к охраняемой законом компьютерной информации» (ч. 1 ст. 272 УК РФ);

2) совершающими неправомерный доступ группой по предварительному сговору или организованной группой (ч. 3 ст. 272 УК РФ);

[2] Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М.: Норма, 2015. – С. 330.
[3] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – № 10. – С. 24-25.

3) совершающими неправомерный доступ, используя для этого свое служебное положение (ч. 3 ст. 272 УК РФ);

4) имеющими право доступа к ЭВМ, системы ЭВМ или их сети, но использующими это право в целях достижения преступного результата (уничтожение, блокирование, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети).

Диспозиция ст. 273 УК РФ аналогично не содержит в себе указания на форму вины. При анализе данного состава преступления необходимо обратиться к ч. 2 ст. 24 УК РФ, говорящей о том, что деяние признается совершенным по неосторожности, лишь в том случае, когда это оговорено соответствующей нормой УК РФ. Это подтверждает нашу точку зрения касательно того, что преступления, предусмотренные ст. 273 УК РФ, совершаются исключительно с формой вины в виде прямого умысла.

Субъект преступления по ч. 1 ст. 273 УК РФ общий, т.е. субъектом данного преступления может быть любой гражданин, достигший шестнадцати лет.

Ч. 2 в качестве субъектов называет «совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности». Появление с 2011 года в качестве специального субъекта, использующего служебное положение, было заимствовано из ст. 272 УК РФ[4].

В ч. 3 предусмотрено наступление тяжких последствий или создание угрозы их наступления. В таком случае состав преступления является материальным, то есть деяние окончено с момента наступления общественно опасных последствий, а если создана угроза их наступления, то состав является усеченным.

Тяжесть последствий устанавливается с учетом всей совокупности обстоятельств дела (причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование,

[4] Евдокимов К.Н. Актуальные проблемы совершенствования субъекта состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Сибирский юридический вестник. – 2013. – № 3. – С. 71.

модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и др.)[5].

Субъективная сторона в таком случае характеризуется двумя формами вины – умыслом по отношению к самому деянию и неосторожностью по отношению к последствиям.

Субъективную сторону части 1 ст. 274 УК РФ характеризует наличие умысла, направленного на нарушение правил эксплуатации ЭВМ.

Субъект данного преступления – специальный, это лицо в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

Данное преступление может совершаться как умышленно, так и по неосторожности.

Часть 2 – состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление тяжких последствий или создание угрозы их наступления. Содержание последних, очевидно, аналогично таковому для ч. 2 ст. 273 УК РФ.

Субъектом преступлений, предусмотренных ч. 1-2 ст. 274.1 УК РФ, является физическое вменяемое лицо, достигшее возраста 16 лет. Субъектом ч. 3 ст. 274.1 УК РФ может быть, как общий – в части правил доступа к ресурсам, так и специальный – в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включенные в соответствующий реестр.

При неправомерном доступе (ч. 2 ст. 274.1 УК РФ) умысел может быть, как прямым, так и косвенным.

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа может совершаться как умышленно, так и по неосторожности.

[5] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] – Режим доступа: https://genproc.gov.ru/documents/nauka/execution/document104550 (дата обращения: 03.03.2022).

Под лицами, использующими свое служебное положение, в ч. 4 ст. 274.1 УК РФ следует понимать лиц, осуществляющих организационно-распорядительные или административно-хозяйственные обязанности в организации, иных лиц. В организации признаками такого лица могут обладать: руководители организации или ее подразделений и работники, уполномоченные на решение задач по информационной безопасности, а также иные лица, выполняющие на основании гражданско-правовых договоров задачи по обеспечению безопасности КИИ[6].

Исходя из того, что к субъектам КИИ относятся российские юридические лица, которым принадлежат данные системы, в случае передачи ими КИИ на баланс аутсорсинговой компании, сделавшая это, например, нефтяная компания под определение субъекта КИИ не подходит, и поэтому ее сотрудники (руководители) не могут быть исполнителями преступления, предусмотренного ч. 3 ст. 274.1 УК РФ.

Вместе с тем, если такая организация передала КИИ на аутсорсинг, но у нее остались компьютеры, через которые можно удаленно подключаться к КИИ, ее следует считать субъектом КИИ, а ее сотрудников – субъектами рассматриваемых преступлений несмотря на то, что непосредственно соответствующей КИИ она не владеет.

Анализ признаков составов преступлений, предусмотренных ч. 3-5 ст. 274.1 УК РФ, позволил сформулировать положения по квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации ее владельцами и эксплуатантами.

Так, диспозиция ч. 3 данной статьи включает противоправные деяния в форме как активного действия, так и бездействия в отношении соблюдения правил эксплуатации и доступа к объектам КИИ.

Обязательным признаком составов рассматриваемых преступлений является наступление общественно опасных последствий: причинение вреда КИИ РФ (ч. 3 и 4) и тяжкие последствия, имеющие значение для ее безопасности (ч. 5).

Субъект (исполнитель) данного преступления – специальный (владелец/эксплуатант КИИ), имеющий доступ к КИИ РФ либо к относящимся к ней объектам в силу исполнения своих служебных обязанностей и обязанный исполнять установленные правила эксплуатации, доступа к КИИ.

[6] Шульга А.В., Галиакбаров Р.Р. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274. 1. УК РФ) // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 5. – С. 239.

Тяжкие последствия (ч. 5) в отличие от вреда (ч. 3) могут распространяться как на объекты КИИ, так и на деятельность субъектов КИИ. Такие последствия могут иметь значение для безопасности КИИ – защищенности, обеспечивающей ее устойчивое функционирование при проведении в отношении ее компьютерных атак, в том числе противоправном нарушении эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации) [7] . Например, причинение организации (субъекту КИИ) материального ущерба, репутационного вреда или возникновение иных негативных для нее последствий; нарушение технологических и бизнес-процессов организации.

В случае с КИИ тяжкие последствия не должны ограничиваться материальным ущербом, например, при остановке воздушного сообщения можно говорить о наступлении тяжких последствий, учитывая критерий массовости, т. е. когда нарушаются права и свободы большого количества субъектов права, когда в результате компьютерного инцидента появляются пострадавшие люди, которые не смогли вовремя вылететь из аэропорта, лишились билетов, самолеты не смогли сесть на аэродром и т. п. В случае отказа системы и, как следствие, прерывания какого-то технологического процесса (например, атомной электростанции) финансовые и другого рода потери будут исчисляться в миллиардах рублей.

Одновременно с этим к тяжким последствиям можно отнести гибель и серьезные травмы людей, разрушения и уничтожение информационной инфраструктуры, нанесение вреда безопасности государства и т. д. То есть тяжесть последствий должна определяться с учетом причинения (или реальности созданной угрозы) тяжкого вреда здоровью людей или смерти, материального ущерба, серьезного нарушения деятельности

[7] Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. – 2019. – № 5. – С. 104.

предприятий, аварий и катастроф, уничтожения, блокирования, модификации или копирования привилегированной информации особой ценности.

Как показало наше исследование, преступления в сфере компьютерной информации имеют сложную формулировку и состав. Как следствие, для эффективной борьбы с киберпреступностью необходимо в первую очередь создать полноценную криминалистическую методику, отвечающую современным достижениям науки и техники. Безусловно, ученые и практические работники еще не раз столкнутся с трудностями теоретико-практического характера, поскольку киберпреступность растет очень быстрыми темпами.

Список литературы

1. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – № 10. – С. 22-25.

2. Евдокимов К.Н. Актуальные проблемы совершенствования субъекта состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Сибирский юридический вестник. – 2013. – № 3. – С. 69-75.

3. Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М.: Норма, 2015. – 688 с.

4. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. – 2019. – № 5. – С. 102-106.

5. Шульга А.В., Галиакбаров Р.Р. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274. 1. УК РФ) // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 5. – С. 238-242.

Автор: Поваляева Лариса Васильевна, Уманец Инна Витальевна
Должность: воспитатель, учитель начальных классов
Образовательное учреждение: МБОУ "Начальная школа-детский сад №44"
Населённый пункт: Белгород, Белгородская область
Тема: Индивидуальная работа с детьми дошкольного и младшего школьного возраста.
Раздел образования: Общеобразовательная организация

Психофизическое развитие любого ребёнка, становление его личности происходит индивидуально. Особенности характера оказывают большое влияние на развитие умений и навыков, усвоение новых знаний. Далеко не все дети могут полноценно работать в группе, в классе, многие нуждаются в индивидуальных занятиях. Задача педагога при проведении таких занятий – помочь каждому воспитаннику и обучающемуся развить свои способности, получить необходимую сумму знаний и навыков, научить ребёнка бороться с излишней застенчивостью или скромностью, поверить в собственные силы [3:12]. В особом внимании нуждаются воспитанники и обучающиеся, которые по каким-либо причинам отстают от группы или класса (часто отсутствуют на занятиях, медлительные, застенчивые, слишком активные) или, наоборот, опережают остальных детей по объёму изученного материала. Отстающим дошкольникам и младшим школьникам индивидуальные занятия позволяют приобрести знания и навыки, соответствующие уровню знаний основной группы или класса.

Индивидуальная работа с детьми делится на четыре группы: коррекционную, компенсирующую, дополнительную, развивающую [1:10].

Коррекционную работу ведут с детьми, имеющими некоторые нарушения в развитии. Очень важным тут является то, что такую работу ведут исключительно квалифицированные специалисты: логопед, психолог, инструктор по физкультуре. Следует отметить, что такая работа ведется с ведома и согласия родителей ребенка.

Компенсирующие занятия проводятся воспитателем и учителем на основе мониторинга с детьми, долго не посещающими детский сад или школу по разным причинам и вследствие чего отставшими от основной части группы или класса.

Дополнительная работа проводится с детьми, которые показывают повышенный интерес к определенным видам знаний или деятельности. Таким детям рекомендуется посещать кружки и дополнительные занятия по интересующим видам деятельности.

Развивающие занятия проводятся наиболее часто. Обычно они проводятся со всеми детьми по очереди для закрепления и повторения того, что дети узнали во время непосредственной образовательной деятельности.

В организации индивидуальной работы могут использоваться следующие приёмы:

- индивидуальное взаимодействие с воспитателем, учителем или узким специалистом (проведение индивидуального занятия, организация которого может включать любые педагогические методы, соответствующие возрасту ребёнка);
- выполнение задания на примере, по образцу педагога (во время самостоятельной деятельности детей, если у ребёнка что-то не получается, педагог демонстрирует алгоритм действий);
- выполнение по образцу или при помощи сверстников (можно создавать пары или микрогруппы детей, где один из ребят нуждается в поддержке; такая организация работы полезна и для ребёнка, исполняющего роль педагога, поскольку учит его умению объяснять и обучать) [2:17].

Приёмы, которые применяет педагог в индивидуальной работе с дошкольниками и младшими школьниками, очень разнообразны: словесные (рассказ, беседа, напоминание, вопрос, проговаривание), наглядные (показ иллюстраций, макетов, предметов), практические (упражнение, совместно выполнение действий, моделирование, эксперимент).

Все дети, как известно, разные, и каждый ребёнок имеет право на собственный путь развития. Поэтому в учебном учреждении должны быть созданы условия для воспитания и обучения детского коллектива в целом, а также каждому воспитаннику и обучающемуся предоставлена возможность проявить индивидуальность и творчество [3:45].

В своей работе воспитатель детского сада и учитель начальных классов в первую очередь опираются на основные положения и требования ФГОС ДО и НОЛ в которых указывается на свободу и пластичность развития ребёнка. ФГОС акцентирует внимание на индивидуализации дошкольного и начального общего образования.

В связи с этим от педагога требуется быть не только профессионалом, знающим психологию и физиологию дошкольника и младшего школьника, но и чутким, внимательным товарищем, уважающим интересы маленького человека, признающим его право на собственное мнение, свой личный темп и особенности развития. Осуществить эти требования поможет рационально организованная индивидуальная работа с детьми.

Литература

1. Вагурина Л. Учись, играя! (Пособие для занятий с детьми дошкольного возраста) / Л. Вагурина. – Москва: РГГУ, 2015. – 51 с.
2. Панфилова М.А. Игротерапия общения. М.: «Гном и Д», 2001. – 64 с.
3. Петрова Л.И. Индивидуальный подход в воспитании младших школьников / Л.И. Петрова. - М.: Феникс, 2007. – 336 с.
4. Свирская Л. Шпаргалки для родителей//Детский сад со всех сторон. 2002 г. – 147 с.